INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA

DE INGENIERIA Y CIENCIAS SOCIALES Y ADMINISTRATIVAS

"ANÁLISIS Y DESCRIPCIÓN DE IDENTIFICACIÓN POR RADIO FRECUENCIA: TECNOLOGÍA, APLICACIONES, SEGURIDAD Y PRIVACIDAD"

T E S I S

QUE PARA OBTENER EL TITULO DE
LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

P R E S E N T A

ALBERTO RODRÍGUEZ HERNÁNDEZ

MEXICO D.F. **2009**

SECRETARIA
DE
EDUCACION PUBLICA

INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA Y CIENCIAS SOCIALES Y ADMINISTRATIVAS

AV. TE 950 COL. GRANJAS MÉXICO C.P. 08400 IZTACALCO, D.F.
CONMUTADOR 56-24-20-00 TEL/FAX. Ext. 42006

JEFATURA DE LA CARRERA DE CIENCIAS DE LA INFORMÁTICA
S.Aca.JCLCI.316.2009

"2009, Año de la Reforma Liberal"
"2009 Año Internacional de la Astronomía"
"75 Aniversario de la Escuela Nacional de Ciencias Biológicas"
"50 Aniversario de XEIPN Televisión Canal Once"
"50 Aniversario de la Unidad Profesional Adolfo López Mateos"

27 de mayo de 2009

ASUNTO: Autorización del tema de titulación
OPCIÓN: Tesis

C. PASANTE:
ALBERTO RODRÍGUEZ HERNÁNDEZ
P R E S E N T E

Por este medio, me permito comunicarles que ha sido autorizado su informe de Titulación denominado: **"ANÁLISIS Y DESCRIPCIÓN DE IDENTIFICACIÓN POR RADIO FRECUENCIA: TECNOLOGÍA, APLICACIONES, SEGURIDAD Y PRIVACIDAD."**

Con el siguiente contenido:

El informe será dirigido por el Ing. Abel Meléndez Manrique

A T E N T A M E N T E
"LA TÉCNICA AL SERVICIO DE LA PATRIA"

LIC. DANIEL OSWALDO RICO ARAGÓN
JEFE DE CARRERA CSAS. DE LA INFORMÁTICA

JEFATURA DE CARRERA DE CIENCIAS DE LA INFORMÁTICA
I. P. N.
UPIICSA
SUBDIRECCIÓN ACADEMICA

c.p. Interesados
Expediente.
DORA/*Ray**

INDICE

Capitulo 5 Aplicaciones

Capitulo 6 Seguridad y Privacidad

Capitulo 7 Regulación y Estandarización

Capitulo 8 Implementación de Sistemas de Control de Acceso RFID

Resumen

RFID es, sin duda una de las tecnologías de auto identificación que ha experimentado un crecimiento más acelerado y sostenido en los últimos tiempos. Las posibilidades que ofrece la lectura a distancia de la información contenida en una etiqueta, sin necesidad de contacto físico, junto con la capacidad para realizar múltiples lecturas (y en su caso, escrituras) simultáneamente, abre la puerta a un conjunto muy extenso de aplicaciones en una gran variedad de ámbitos, desde la trazabilidad y control de inventario, hasta la localización y seguimiento de personas y bienes, o la seguridad en el control de accesos.

Consiste en aplicar la radio frecuencia para la identificación, por lo que nos permite identificar objetos mediante ondas de radio. Es un paso hacia delante para las tecnologías de identificación automática y una clara alternativa a sistemas tradicionales de control y rastreo de objetos o personas.

Son muchas las grandes compañías que apoyan la implantación y el uso sensato de la RFID, por lo que se puede esperar que su futuro sea muy prometedor. No hay duda de que se trata de una tecnología que puede aportar sustanciales ventajas en muchos ámbitos de aplicación. Sin embargo, el éxito final en la implantación de esta tecnología está sujeto a la superación de una serie de obstáculos, entre los que es necesario destacar los aspectos de seguridad y privacidad

El presente trabajo se enfoca en un profundo análisis de la tecnología de Identificación por Radio Frecuencia, RFID es por este motivo que se inicia con un panorama general de ella pasando por sus aspectos físicos y técnicos, frecuencias, tecnología, normatividad y legislación en la materia

Introducción

En la actualidad, dado el avance y rápido desarrollo de la tecnología, y en particular de la microelectrónica, es muy común el uso de dispositivos y elementos electrónicos portátiles de mediano y alto valor.

Para esto se están implementando estrategias para brindar seguridad sobre estos elementos, lo cual no es fácil de garantizar, dado el tamaño cada vez menor y el uso, día a día, más frecuente al cual están siendo sometidos.

Dada la importancia que se le ha dado actualmente al tema de seguridad para controlar al personal de una institución, se han implementado, a través de diferentes tecnologías, sistemas que responden a las necesidades de los clientes que, cada vez demandan más y mejores servicios en este aspecto.

Para todo esto, en la actualidad, en casi cualquier organización de nuestro país se debe recurrir al registro de entrada y salida de personal que ahí de manera casi manual o con el uso de tarjetas que son pasadas por un reloj checador.

Sin embargo, todas estas estrategias presentan falencias como la necesidad de realizar procesos de manera manual, así como la falsificación o alteración del registro de entradas y salidas.

Por esta razón, se inició la búsqueda de alternativas tecnológicas prácticas y relativamente económicas para implementar una posible solución al problema mencionado. Se consideró la utilización de dispositivos RFID (Radio Frequency Identification), una tecnología de identificación por radiofrecuencia, constituido por un pequeño circuito, con una antena integrada. Al recibir energía vía radio desde un emisor externo, el dispositivo responde con una señal que indica su estado. Su principal ventaja es que detecta los equipos que incorporen este sistema, de manera inalámbrica y sin requerimientos de línea de vista.

Se adquirió un dispositivo lector de RFID Phidget así como Tags para realizar las pruebas. Se asignaron los códigos de las tags a registros de una base de datos SQL Server ya que se trabajo bajo la plataforma .Net de Microsoft.

Por otro lado, se desarrollo e implementó una aplicación, la cual se encarga de manejar el hardware y coordinar el proceso de autenticación de los usuarios registrados en la base de datos. Dicha aplicación se desarrollo en C# y la base de datos en SQL Server.

1. Presentación

1.1 Caso de Estudio

El análisis que se hace en este trabajo surge a partir de la implementación que están dando diversos sectores tanto industriales como gubernamentales en varios países incluyendo el nuestro. Aunque esto no significa que estudiantes o investigadores principalmente en América Latina cuenten con suficiente información que les sirva como apoyo en trabajos futuros enfocados en implementar o enriquecer la tecnología RFID que se encuentra en constante evolución.

Así mismo la propuesta para implementar un sistema de control de acceso de personas y vehículos usando RFID surge como necesidad de contar con un sistema de este tipo donde se contempla el uso de tecnología de punta, la escalabilidad, confiabilidad y seguridad.

Una ventaja del uso de estas tarjetas electrónicas es que no necesitan contacto físico con algún hardware; sólo con aproximarla a cierta distancia del lector, la tarjeta será validada inclusive a varios metros los lectores pueden detectar las tarjetas de las personas y vehículos, permitiendo o denegando el acceso según las políticas previas de seguridad de cada organización.

1.2 Objetivo General

Profundo estudio de la tecnología RFID en sus diferentes frecuencias desde sus características físicas y técnicas hasta su legislación y estandarización internacional así como una propuesta de aplicación para el control de acceso de personal.

1.3 Objetivos Particulares

- Conocer los fundamentos de operación, características físicas, técnicas, normas y legislación de los Sistemas RFID
- Implementar un sistema RFID de control de acceso de personal que trabaje a una frecuencia de 125Khz.
- Implementar la interfaz de Comunicación de Información RFID con la PC bajo la tecnología .Net de Microsoft
- Desarrollar una Aplicación de Identificación de Personal para probar la Interfaz de Comunicación de Información RFID

1.4 Justificación

Las tecnologías de la información (IT) tienen una gran influencia en las organizaciones actuales y además aporta muchas innovaciones a la estructura industrial y de negocios, así como información sobre comportamiento del consumidor.

En la estructura industrial y de negocios actual, el mercado está siendo digitalizado, en el sentido que todos los datos de logística, compras, producción, ventas y distribución son utilizados para brindar información más precisa y de este modo incrementar la eficiencia en toda la cadena de valor. Por tal motivo es que con el paso del tiempo van surgiendo nuevas y cada vez más sofisticadas tecnologías que ayudan a la Industria a obtener dicha información.

Es por tal motivo que la tecnología no solo va surgiendo de manera veloz sino que también va evolucionando de la misma manera para cumplir con las exigencias del mercado.

Específicamente la tecnología RFID parece estar tecnológicamente madura, aunque se halla inmersa en una continua evolución y mejora de sus prestaciones, como evidencia el número cada vez mayor de patentes y software que complementa el uso de esta tecnología. Las etiquetas son cada vez más pequeñas y su capacidad de almacenamiento continúa en aumento, las antenas son más eficientes y potentes permitiendo alcanzar rangos de cobertura mayores, los algoritmos de seguridad son cada vez más robustos y con ello van surgiendo nuevas aplicaciones innovadoras.

Ha habido diversos casos de éxito en la implantación de sistemas de RFID, especialmente en actividades relacionadas con la logística, la distribución y el control y rastreo de personas o animales, como ejemplo grandes distribuidores como Walmart© y Guillette® han optado por utilizar la tecnología RFID en sucursales de Estados Unidos y Europa. Igualmente, en muchos aeropuertos han implantado un sistema RFID para la gestión de las maletas. También hay empresas cuyo personal está equipado con una tarjeta RFID para su identificación y gestión de zonas autorizadas o restringidas.

Otro ejemplo del uso de esta tecnología en el control de acceso se da en las instalaciones del Ejército de los Estados Unidos, que realiza pruebas para identificación de vehículos, automatizando esta tarea sin sacrificar seguridad otro ejemplo del uso de esta tecnología es en la Enterprise Charter School[1] en Búfalo, NY, donde utilizan RFID como medio para identificar y tener control de acceso a edificaciones. Esta escuela pública utilizará también esta tecnología para

[1] 275 Oak Street. Buffalo, New York 14203. Tel. (716) 855-2114

identificar y proteger los activos de esta (entre los cuales se encuentran libros de biblioteca, computadoras portátiles, vehículos y otros ítems).

Además de esto, los estudiantes pueden realizar compras en la cafetería con sus tarjetas de identificación.

Como se puede apreciar la tecnología RFID está siendo adoptada cada vez mas por la industria debido a que su costo se ha venido reduciendo al paso del tiempo y sus capacidades son mayores. Esto permite generar grandes incrementos en la productividad y administración principalmente en los sectores de cadenas de suministro, transporte, seguridad y control de inventarios y personal.

Es a partir de esta visión que el presente trabajo tiene como finalidad realizar un estudio profundo sobre la situación actual de la tecnología de Identificación por Radiofrecuencia (RFID por sus siglas en inglés) para que estudiantes e investigadores interesados en la materia cuenten con información suficiente y confiable que les ayude a visualizar el alcance de esta tecnología.

Además pretende mostrar las ventajas del uso de esta tecnología en la implementación de un sistema de control de acceso para personas que permita dar una visión sobre el uso de este tipo de sistemas.

1.5 Limites y Alcances

La principal finalidad de esta investigación es conocer la tecnología RFID a fondo desde sus bases físicas y metódicas hasta las normatividad que han dispuesto la ISO y EPC, en lo concerniente a este tipo de tecnología de Auto – Identificación. Así mismo se realiza una implementación de control de acceso RFID y se desarrolla la aplicación para poder gestionar las tags del sistema RFID.

En este estudio no se pretende la fabricación de ningún componente RFID, ya que se necesaria de un estudio único sobre el tema, aunque a partir de esta tesis se puede continuar con una amplia investigación sobre manufactura de componentes RFID puesto que dicha investigación va más allá de las generalidades sobre tecnología RFID.

2. Introducción a la Tecnología RFID

La tecnología de Identificación por Radiofrecuencia (RFID) es un sistema de auto identificación inalámbrica, el cual consta de etiquetas que almacenan información y lectores que pueden leer a estas etiquetas a distancia utilizando una frecuencia de onda electromagnética para realizar dicha tarea. Estas frecuencias varían según la aplicación y puede ser de 125Khz, 13.56Mhz, 433-860-960MHz, 2,45GHz y 5.8Ghz

Esta tecnología a existido desde hace mas de 50 años sin embargo el uso que se le daba no era el que en las ultimas dos décadas se le esta dando, puesto que era de uso exclusivo de la milicia y sus costos eran muy elevados.

En la última década se ha retomado su estudio y se le ha dado infinidad de usos fuera del ámbito militar lo que ha permitido que sea adoptada cada vez por la industria debido a que su costo es cada vez menor y sus capacidades son mayores, permitiendo generar grandes beneficios como incrementos en la productividad y la administración principalmente en los sectores de cadenas de suministro, transporte, seguridad y control de inventarios.

El avance cada vez mayor de esta tecnología de identificación automática (Auto-Id) sobre otras del mismo grupo se debe principalmente a que no se necesita el contacto visual entre una etiqueta comúnmente llamada tag y un lector para realizar la lectura de la información como en el caso de su principal competidor, el código de barras [1].

Otras ventajas sobresalientes sobre su competidor es que se puede almacenar y sobrescribir mucha mas información en una tag que en un sencillo código de barras, así mismo las etiquetas electrónicas pueden ser leídas de manera simultánea y el código de barras debe ser leído de manera secuencial.

Estudios realizados sostienen que RFID puede proporcionar ventajas estratégicas en muy diversas áreas de negocio, proporcionando seguimiento preciso en tiempo real de la cadena de suministro de bienes o materias primas, y en general la posibilidad de monitorización en tiempo real de los activos o personal de una empresa.[2] En la actualidad su uso va en incremento principalmente en aplicaciones para control de acceso de personas, rastreo de individuos, objetos y animales, gestionar la materia prima de los almacenes, las maletas en los aeropuertos, las visitas de pacientes en hospitales, los sistemas de préstamo en bibliotecas e incluso para la programación de los sistemas de locomoción de robots para la industria en general, entre otras muchas aplicaciones.

Parámetros	Código de Barras	OCR	Reconocimiento de Voz	Biométrica	Tarjetas Inteligentes	RFID
Cantidad de Datos (Bytes)	1-100					
Densidad de Datos	Baja	Baja	Alta	Alta	Muy Alta	Muy Ala
Legibilidad de los Lectores	Buena	Buena	Cara	Cara	Buena	Buena
Legibilidad ante las personas	Limitada	Simple	Simple	Difícil	Imposible	Inaccesible
Influencia de la Cubierta	Falla Total	Falla Total	---------	Posible	---------	No Influye
Influencia por dirección/Posición	Baja	Baja	---------	---------	Unidimensional	No Influye
Costo de Operación	Bajo	Bajo	Ninguno	Ninguno	Médium	
Rapidez de Lectura	Baja 4s	Baja 3s	Muy Baja 5s	Muy Baja 5-10s	Muy Baja 4s	Muy Rápida 0-5ms
Distancia Máx. entre el lector y el dispositivo.	0-50cm	1cm	0-50cm	Contacto Directo	Contacto Directo	0-5m

Tabla 2.1 Diferencias entre las principales tecnologías de Identificación Automática

2.1 Antecedentes de la tecnología RFID

Antes de hablar plenamente de la tecnología RFID hay que señalar que dicha tecnología está fuertemente ligada con los trabajos de James Clerk Maxwell[1], Heinrich Rudolf Hertz[2] y Guglielmo Marconi[3] ya que trabaja totalmente de manera inalámbrica, en una frecuencia determinada en el espectro electromagnético así mismo utiliza ondas de radio para realizar la lectura de las Tags.

Sus orígenes surgen durante la Segunda Guerra Mundial en la cual se desarrollo la tecnología del transpondedor de IFF, Identification, Friend or Foe. Desarrollada por el ejército Británico para identificar a los aeroplanos como amigos o enemigos que sobrevolaban el Canal de la Mancha, el sistema utilizaba un equipo que los aviones aliados llevaban a bordo (nombre en código "loro", Parrot) y que emitía señales codificadas.

[1] Edimburgo, 13 de junio de 1831- Cambridge, Reino Unido, 5 de noviembre de 1879. Físico escocés conocido principalmente por haber desarrollado la teoría electromagnética clásica, sintetizando todas las anteriores observaciones, experimentos y leyes sobre electricidad, magnetismo y aun sobre óptica, en una teoría consistente

[2] 22 de febrero de 1857 - 1 de enero de 1894. Físico alemán por el cual se nombra al hercio, la unidad de frecuencia del Sistema Internacional de unidades (SI). En 1888, fue el primero en demostrar la existencia de la radiación electromagnética construyendo un aparato para producir ondas de radio.

[3] Bolonia, 25 de abril de 1874 - Roma, 20 de julio de 1937. ingeniero eléctrico italiano y ganador del Premio Nobel de Física en 1909, conocido por el desarrollo de un sistema de telegrafía sin hilos (T.S.H.) o radiotelegrafía

El radar secundario de vigilancia o Secondary Surveillance Radar, SSR es el desarrollo civil del sistema IFF militar, de hecho, los sistemas IFF que llevan a bordo los aviones militares modernos son compatibles con el SSR

Terminada la guerra, los científicos e ingenieros continuaron sus investigaciones sobre estos temas. En octubre de 1948, Harry Stockman publicó un artículo en Octubre de 1948 en Proceedings of the IRE (Revista Editada por el IEEE) titulado "Communications by Means of Reflected Power", que se puede considerar como la investigación más cercana al nacimiento de RFID. Fue a partir de ese momento, el desarrollo de la tecnología RFID ha sido lento pero constante.

Durante la década de los 50 se realizaron multitud de estudios relacionados con la tecnología, principalmente orientados a crear sistemas seguros para su aplicación en minas de carbón, explotaciones petrolíferas, instalaciones nucleares, controles de acceso o sistemas antirrobo.

Durante esta época se publicaron dos artículos importantes: "Applications of Microwave Homodyne", de F. L. Vernon, y "Radio Transmission Systems with Modulatable Passive Responders", de D. B. Harris.

En los años 60 se profundizó en el desarrollo de la teoría electromagnética y empezaron a aparecer las primeras pruebas de campo, apareció la activación remota de dispositivos con batería, la comunicación por radar o los sistemas de identificación interrogación-respuesta". Así mismo aparecieron las primeras invenciones con vocación comercial, como "Remotely Activated Radio Frequency Powered Devices", de Robert Richardson, "Communication by Radar Beams" de Otto Rittenback, "Passive Data Transmisión Rechniques Utilizing Radar Beams" de J. H. Vogelman, y "Interrogator-Responder Identification System", de J. P. Vinding.

Además, comenzaron las primeras actividades comerciales. Se fundaron Sensormatic® y Checkpoint®, que junto con otras compañías, desarrollaron un equipo de vigilancia electrónica anti-intrusión denominado EAS (Electronic Article Surveillance). EAS fue el primer desarrollo de RFID y el que indiscutiblemente se ha venido utilizando más ampliamente. Fue el preludio de la explosión de esta tecnología.

Al referirse a la evolución del RFID en la década de los 70, Manish Bhuptani [3] sostiene lo siguiente:

> Durante los años 70 desarrolladores, inventores, fabricantes, centros de investigación, empresas, instituciones académicas y administración realizaron un activo trabajo de desarrollo de la tecnología, lo que redundó en notables avances, apareciendo las primeras aplicaciones de RFID. A pesar de ello, la tecnología se siguió utilizando de modo restringido y controlado. Grandes empresas como Raytheon, RCA y Fairchild empezaron a desarrollar

tecnología de sistemas de identificación electrónica, y en 1978 ya se había desarrollado un transpondedor pasivo de microondas.

A finales de esta década ya se había completado una buena parte de la investigación necesaria en electromagnetismo y electrónica para RFID, y la investigación en otros de los componentes necesarios, las tecnologías de la información y las comunicaciones, estaba empezando a dar sus frutos, con la aparición del PC y de ARPANET

En los años 80 aparecieron nuevas aplicaciones. Fue la década de la completa implementación de la tecnología RFID. Los principales intereses en Estados Unidos estuvieron orientados al transporte, al acceso de personal y, más débilmente, a la identificación de animales. En Europa sí cobró un especial interés el seguimiento de ganado con receptores de identificación por radiofrecuencia como alternativa al mercado.
Más tarde también aparecieron los primeros peajes electrónicos. La primera aplicación para aduanas se realizó en 1987, en Noruega, y en 1989 en Dallas. Todos los sistemas eran propietarios, y no existía la interoperabilidad.

En los primeros años de los 90 se inició el uso en EEUU del peaje con control electrónico, autopistas de Houston y Oklahoma incorporaban un sistema que gestionaba el paso de los vehículos por los pasos de control. En Europa también se investigó este campo y se usaron sistemas de microondas e inductivos para controles de accesos y billetes electrónicos. Un nuevo avance en el mundo del automóvil vino con la tecnología RFID de la mano de Texas Instruments© (TI), un sistema de control de encendido del automóvil. Apareció también un sistema de Philips que permitía la gestión del encendido, control del combustible, y control de acceso al vehículo entre otras acciones. Aplicaciones para autopistas y billetes electrónicos se fueron extendiendo por Asia, África, Suramérica y Australia. A partir de aquí el éxito de la tecnología RFID en estos campos hizo que se aplicaran a otros segmentos económicos.

Fue en Dallas por primera vez cuando con un solo tag era utilizado para el acceso a una autopista, al campus universitario, a diferentes garajes de la ciudad, incluido el del aeropuerto. El avance de la tecnología durante esta década fue rápido debido a los desarrollos tecnológicos en otros campos que permitían fabricar cada vez equipos más pequeños, con más memoria, con más alcance y abaratando su costo de fabricación apareciendo así nuevos usos hasta esa fecha descartados.

Y a partir del año 2000, empezó a quedar claro que el objetivo de desarrollo de etiquetas a 0.05 dólares podría alcanzarse, con lo que la RFID podía convertirse en una tecnología candidata a sustituir a los códigos de barras existentes. El año 2003 marcó un hito e importancia en el

desarrollo de la tecnología RFID: Walmart© y el Departamento de Defensa (DoD) estadounidense decidieron adherirse a la tecnología RFID. Les siguieron otros fabricantes, como Target, Procter & Gamble® y Gillette®. En 2003 el centro AutoID se convirtió en EPCglobal, creadora de estándares adoptados por Walmart® y el DoD.
La empresa Texas Instruments desarrolló diversas aplicaciones para el control del encendido del motor del vehículo, control de acceso de vehículos o pases de esquí.
Asimismo, numerosas empresas en Europa se introdujeron en el mercado, más aún tras detectar la potencial aplicación en la gestión de artículos.

En año 2002 empezó a despuntar la tecnología NFC (Near Field Communication), tecnología que mejora las prestaciones de RFID gracias a que incluye un único dispositivo, un emisor y un receptor RFID, y que puede insertarse en un dispositivo móvil, aportando a éste nuevas funcionalidades para un gran número de aplicaciones.

En Europa, el proyecto lanzado en 2005 por Correos de España, Q-RFID, liderado por ©AIDA Centre SL, ha contribuido a incorporar las últimas tecnologías de control por radiofrecuencia para permitir la trazabilidad de la correspondencia a lo largo de todo el proceso postal. QRFID ha resultado uno de los más importantes proyectos de RFID de Europa, suponiendo una gran contribución al desarrollo e implantación de la tecnología. Aunque el proyecto ha finalizado en 2007, el éxito alcanzado garantiza la continuidad del mismo.

Todo hace pensar que en los próximos años la tecnología RFID va camino de convertirse en una tecnología ampliamente utilizada en multitud de sectores. El creciente interés en el comercio electrónico móvil traerá consigo más aplicaciones, gracias a la capacidad de RFID para transportar datos que pueden ser capturados electrónicamente.

El futuro de RFID parece ser esperanzador, en un mundo basado en el poder de la información y donde cada vez se desecha más el cable, el radio de acción de esta tecnología parece ser bastante grande. El interés por el comercio virtual parece que tiene su principal valedor en estos sistemas en los que basar una correcta gestión de todo el proceso. Por ese motivo la FCC (Federal Communications Commission) escogió el espectro entorno de los 5,9 GHz para nuevos sistemas inteligentes de transporte y para las nuevas aplicaciones que necesiten. Pero para estas nuevas aplicaciones se necesita un gran desarrollo de la tecnología. El futuro de RFID parece alentador, pero como todas las tecnologías necesita de los otros campos tecnológicos para avanzar.

2.2 Que es un sistema RFID

Un sistema de RFID (Radio Frequency IDentification) es la tecnología inalámbrica que nos permite, básicamente, la comunicación entre un lector y una etiqueta. Estos sistemas permiten almacenar información en sus etiquetas mediante comunicaciones de radiofrecuencia. Esta información puede ir desde un Bit hasta KBytes, dependiendo principalmente del sistema de almacenamiento que posea el transponder.

La Identificación por Radio Frecuencia ha recibido mucha atención recientemente, ya que se cree que la RFID puede revolucionar la gestión de la cadena de suministro, como complemento de los códigos de barras con el objeto de crear un sistema de seguimiento. Varios de los principales operadores de la cadena de suministro y minoristas, como Wal-Mart en los Estados Unidos, han desplegado sistemas RFID en algunos puntos de sus cadenas de suministro [4].

Esto tuvo resultados fascinantes por lo que algunas otras tiendas están pensando en implantarlo a gran escala sin embargo hay ciertas cuestiones que deben ser resueltas para prevenir riesgos y mejorar la tecnología como tal.

Una de las claves de esta tecnología es que la recuperación de la información contenida en la etiqueta se realiza vía radiofrecuencia y sin necesidad de que exista contacto físico o visual (línea de vista) entre el dispositivo lector y las etiquetas, aunque en muchos casos se exige una cierta proximidad de esos elementos.

Los sistemas de RFID tienen multitud de aplicaciones. Pueden utilizarse como tarjetas identificadotas sin contacto, un uso de este tipo se puede ver por ejemplo en el sistema de pago utilizado en peajes, que permite que el vehículo no tenga que detenerse o en los accesos a edificios oficiales o a empresas privadas. Otra aplicación muy usada son los inmovilizadores de vehículos, que consisten en un sistema interrogador situado en el vehículo a proteger y en un identificador en la llave.

Se pueden usar para identificar envío de cartas o paquetes en agencias de transporte, identificadores de animales, identificadores de equipajes aéreos, gestión de supermercados, inventario automático, distribución automática, localización de documentos, gestión de bibliotecas, etc. Incluso se esta hablando de usar la tecnología RFID para la identificación de personas con libertad vigilada, gente con deficiencias mentales o que se puedan considerar peligrosas para la sociedad. También se están realizando proyectos para incluir chips con el historial médico en personas y en billetes de curso legal para evitar posibles robos y localizar en todo momento el dinero.

2.2.1 Descripción y componentes

RFID (Identificación por Radiofrecuencia) es un método de almacenamiento y recuperación remota de datos, basado en el empleo de etiquetas o “tags” en las que reside la información. RFID se basa en un concepto similar al del sistema de código de barras; la principal diferencia entre ambos reside en que el segundo utiliza señales ópticas para transmitir los datos entre la etiqueta y el lector, y RFID, en cambio, emplea señales de radiofrecuencia (en diferentes bandas dependiendo del tipo de sistema, típicamente 125KHz, 13,56MHz, 433-860-960MHz, 2,45GHz y 5.8Ghz

Todo sistema RFID se compone principalmente de cuatro elementos:

- Una etiqueta RFID, también llamada tag o transpondedor (transmisor y receptor). La etiqueta se inserta o adhiere en un objeto, animal o persona, portando información sobre el mismo. En este contexto, la palabra “objeto” se utiliza en su más amplio sentido: puede ser un vehículo, una tarjeta, una llave, un paquete, un producto, etc. Consta de un microchip que almacena los datos y una pequeña antena que habilita la comunicación por radiofrecuencia con el lector. Los tags son diseñados para que usen una frecuencia que se acople a las necesidades del sistema, que incluyen la distancia de lectura y el ambiente en el que se espera leer el tag. Los tags pueden ser activos (con una batería integrada) o pasivos (sin batería). Los tags pasivos obtienen la energía para operar del campo generado por el lector.

- Un lector o interrogador, encargado de transmitir la energía suficiente a la etiqueta y de leer los datos que ésta le envíe. Consta de un módulo de radiofrecuencia (transmisor y receptor), una unidad de control y una antena para interrogar los tags vía radiofrecuencia.
  Los lectores están equipados con interfaces estándar de comunicación que permiten enviar los datos recibidos de la etiqueta a un subsistema de procesamiento de datos, como puede ser un ordenador personal o una base de datos.
  Algunos lectores llevan integrado un programador que añade a su capacidad de lectura, la habilidad para escribir información en las etiquetas.

- Un ordenador, host o controlador, que aloje la aplicación RFID. Recibe la Información de uno o varios lectores y se la comunica al sistema de información. También es capaz de transmitir órdenes al lector.

- Una antena RFID, Va conectada al lector de RFID, puede ser de varios tamaños y formas, dependiendo de la distancia de comunicación requerida para el desempeño del sistema. La antena activa el tag y transmite los datos emitiendo pulsos.

- Adicionalmente, un Middleware y un sistema ERP de gestión de sistemas IT son necesarios para recoger, filtrar y manejar los datos.

2.2.2 Clasificación de los Sistemas RFID

La clasificación de los Sistemas RFID puede ser muy extensa y puede variar en muchas formas, sin embargo la clasificación más común y más aceptada por varios autores es la que a continuación se menciona:

- Según su capacidad de programación:

- *De sólo lectura*: Las etiquetas se programan durante su fabricación y no pueden ser reprogramadas (solo en casos excepcionales)

- *De una escritura y múltiples lecturas*: Las etiquetas permiten una única reprogramación.

- *De lectura/escritura*: Las etiquetas permiten múltiples reprogramaciones.

- Según el modo de alimentación:

- *Activos*: Las etiquetas requieren de una batería para transmitir la información.

- *Pasivos*: Las etiquetas no necesitan batería.

- Según el rango de frecuencia de trabajo:

- *Baja Frecuencia (LF):* Frecuencia inferiores a 135 KHz.

- *Alta Frecuencia (HF):* Frecuencia de 13.56 MHz.

- *Ultra Alta Frecuencia (UHF):* Frecuencias de 433 MHz, 860 MHz, 928 MHz.

- *Frecuencia de Microondas (Microwave):* Frecuencias de 2.45 GHz y 5.8 GHz.

- Según el protocolo de comunicación:

- *Dúplex:* El transpondedor transmite su información en cuanto recibe la señal del lector y mientras dura ésta. A su vez pueden ser:

- *Half dúplex:* Cuando transpondedor y lector transmiten en turnos alternativos.

- *Full dúplex*: Cuando la comunicación es simultánea. Es estos casos la transmisión del transpondedor se realiza a una frecuencia distinta que la del lector.

- *Secuencial:* el campo del lector se apaga a intervalos regulares, momento que aprovecha el transpondedor para enviar su información. Se utiliza con etiquetas activas, ya que el tag

no puede aprovechar toda la potencia que le envía el lector y requiere una batería adicional para transmitir, lo cual incrementaría el costo.

- Según el principio de propagación:
  - *Inductivos*: Utilizan el campo magnético creado por la antena del lector para alimentar el tag. Opera en el campo cercano y a frecuencias bajas (BF y AF).
  - *Propagación de ondas electromagnéticas*: Utilizan la propagación de la onda electromagnética para alimentar la etiqueta. Opera en el campo lejano y a muy altas frecuencias (UHF, Ultra High Frequency y microondas).

2.2.3 Principio de Funcionamiento

Como hemos visto, existe una gran diversidad de sistemas RFID, los cuales pueden satisfacer un amplio abanico de aplicaciones para los que pueden ser utilizados. Sin embargo, a pesar de que los aspectos tecnológicos pueden variar, todos se basan en el mismo principio de funcionamiento, que se describe a continuación:

1. Se equipa a todos los objetos a identificar, controlar o seguir, con una etiqueta RFID.
2. La antena del lector o interrogador emite un campo de radiofrecuencia que activa las etiquetas.
3. Cuando una etiqueta ingresa en dicho campo utiliza la energía y la referencia temporal recibidas para realizar la transmisión de los datos almacenados en su memoria. En el caso de etiquetas activas la energía necesaria para la transmisión proviene de la batería de la propia etiqueta.
4. El lector recibe los datos y los envía al ordenador de control para su procesamiento.

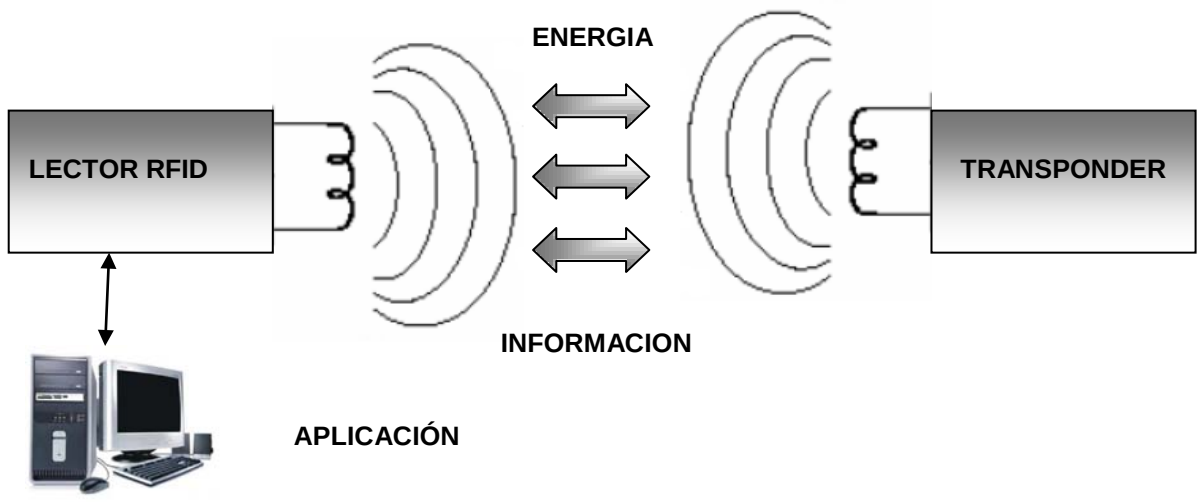


Figura 2.1 Esquema de un sistema RFID

Como podemos ver en la Figura 2.1, existen dos interfaces de comunicación:

• Interfaz Lector-Sistema de Información.

La conexión se realiza a través de un enlace de comunicaciones estándar, que puede ser local o remoto y cableado o inalámbrico como el RS 232, RS 485, USB, Ethernet, WLAN, GPRS, UMTS, etc.

• Interfaz Lector-Etiqueta (tag).

Se trata de un enlace radio con sus propias características de frecuencia y protocolos de comunicación.

Como ya hemos comentado, todo sistema RFID se compone básicamente de cuatro elementos: transpondedor o etiqueta, lector o interrogador, sistema de información y, adicionalmente, middleware. En el presente apartado vamos a proceder a describir cada uno de estos componentes y los principales parámetros que los caracterizan.

2.2.4 Hardware

Uno de los componentes más importantes en los sistemas RFID es sin duda el hardware, pieza fundamental de las aplicaciones RFID.

Sin duda hay que conocer que hardware envuelve un sistema RFID y no solo eso sino también como trabaja, ya que existen diferentes tipos de sistemas que utilizan esta tecnología y no todas utilizan el mismo hardware, todo depende del sistema y el fin que tenga dicho sistema RFDI.

2.2.4.1 Transpondedores

El transpondedor es el dispositivo que va embebido en una etiqueta o tag y contiene la información asociada al objeto al que acompaña, transmitiéndola cuando el lector la solicita.
Está compuesto principalmente por un microchip y una antena. Adicionalmente puede incorporar una batería para alimentar sus transmisiones o incluso algunas etiquetas más sofisticadas pueden incluir una circuitería extra con funciones adicionales de entrada/salida, tales como registros de tiempo u otros estados físicos que pueden ser monitorizados mediante sensores apropiados como sensores de temperatura, humedad, etc.[5]

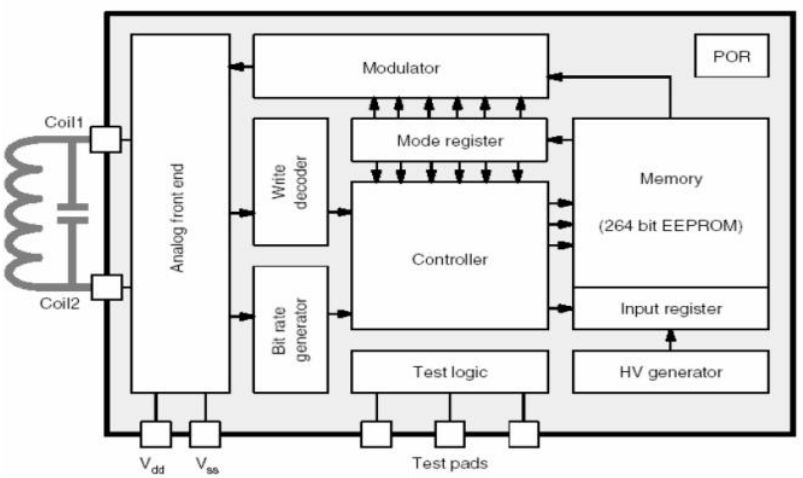


Figura 2.2 Esquema de un transponder de RFID

El microchip incluye:

- Una circuitería analógica que se encarga de realizar la transferencia de datos y de proporcionar la alimentación.

- Una circuitería digital que incluye:
- La lógica de control.
- La lógica de seguridad.
- La lógica interna o microprocesador.

- Una memoria para almacenar los datos. Esta memoria suele contener:

- Una ROM (Read Only Memory) o memoria de sólo lectura, para alojar los datos de seguridad y las instrucciones de funcionamiento del sistema.
- Una RAM (Random Access Memory) o memoria de acceso aleatorio, utilizada para facilitar el almacenamiento temporal de datos durante el proceso de interrogación y respuesta.
- Una memoria de programación no volátil. Se utiliza para asegurar que los datos están almacenados aunque el dispositivo esté inactivo. Típicamente suele tratarse de una EEPROM (Electrically Erasable Programmable ROM). Este tipo de memorias permite almacenar desde 16 bytes hasta 1 Mbyte, posee un consumo elevado, un tiempo de vida (número de ciclos de escritura) limitado (de entre 10.000 y 100.000) y un tiempo de escritura de entre 5 y 10 ms. Como alternativa aparece la FRAM (Ferromagnetic RAM) cuyo consumo es 100 veces menor que una EEPROM y su tiempo de escritura también es menor, de aproximadamente 0.1 µs, lo que supone que puede trabajar prácticamente en tiempo real. En sistemas de microondas se suelen usar una SRAM (Static RAM). Esta memoria posee una capacidad habitualmente entre 256 bytes y 64 kbytes (aunque se

puede llegar a 1Mbyte) y su tiempo de escritura es bajo, pero en contrapartida necesita una batería adicional para mantener la información.

- Registros de datos (buffers) que soportan de forma temporal, tanto los datos entrantes después de la demodulación como los salientes antes de la modulación. Además actúa de interfaz con la antena. La información de la etiqueta se transmite modulada en amplitud (ASK, *Amplitude Shift Keying*), frecuencia (FSK, *Frequency Shift Keying*) o fase (PSK, *Phase Shift Keying*). Es decir, para realizar la transmisión se modifica la amplitud, frecuencia o fase de la señal del lector. Típicamente la modulación más utilizada es la ASK debido a su mayor sencillez a la hora de realizar la demodulación. La frecuencia utilizada por el transpondedor, en la gran mayoría de los casos, coincide con la emitida por el lector. Sin embargo, en ocasiones se trata de una frecuencia subarmónica (submúltiplo de la del lector) o incluso de una frecuencia totalmente diferente de la del lector (no armónica).

La antena que incorporan las etiquetas para ser capaces de transmitir los datos almacenados en el microchip puede ser de dos tipos:

- Un elemento inductivo (bobina).
- Un dipolo.

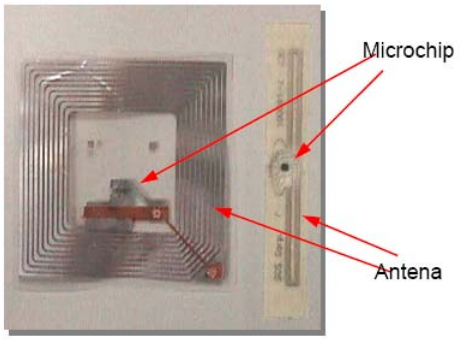


Figura 2.3.Aspecto de los dos principales diseños de una etiqueta (a la izquierda antena inductiva y a la derecha antena dipolar).

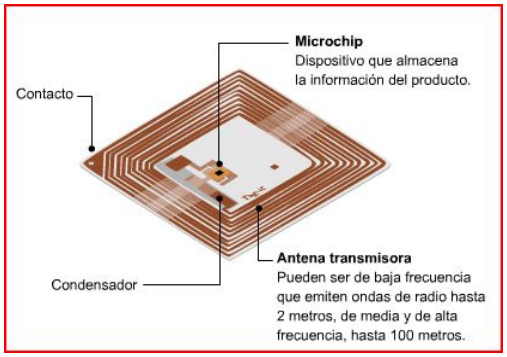


Figura 2.4. Detalle de una antena de un tag.

Los parámetros que caracterizan las etiquetas RFID y comprenden las bases para diseñar sus especificaciones son: el modo de alimentación, la capacidad y tipo de datos almacenados, la velocidad de lectura de datos, las opciones de programación, la forma física y los costos.

Modo de alimentación

Aunque los niveles requeridos para que el transpondedor envíe la información son muy pequeños, del orden de micro a miliwatios, es necesario que las etiquetas dispongan de algún tipo de alimentación. Dependiendo del modo en que éstas obtengan su potencia, las etiquetas se clasifican en activas o pasivas.

Las etiquetas activas, además de recoger energía del lector, se alimentan de una batería.
Normalmente incorporan una pila que posee una alta relación potencia-peso y son capaces de funcionar en un intervalo de temperaturas que va desde -50ºC hasta 70ºC. [6]

Aunque el empleo de baterías implica un tiempo de vida finito para el dispositivo, la colocación de una pila acoplada de forma apropiada a la circuitería de baja potencia, puede asegurar un tiempo de vida de algo más de 10 años, dependiendo también de las condiciones de trabajo en las que se encuentre, es decir, las temperaturas, ciclos de lectura/escritura y su utilización.
Típicamente son dispositivos de lectura/escritura. Además, una ventaja adicional que presentan frente a las etiquetas pasivas es que pueden usarse parar gestionar otros dispositivos, como pueden ser los sensores.
En términos generales las etiquetas RFID activas permiten un radio de cobertura mayor, mejor inmunidad al ruido y tasas de transmisión más altas cuando se trabaja a alta frecuencia. Estas ventajas se traducen en un costo mayor, por lo que se aplican cuando los bienes a identificar lo justifican.

Existen dos tipos de etiquetas activas:

- Aquellas que normalmente se encuentran desactivadas (modo reposo) y se activan (despiertan) cuando un lector las interroga. De esta forma se ahorra batería.
- Aquellas que periódicamente envían señales, aunque un lector no las interrogue. Operan a frecuencias más bajas y a menores tasas de transferencias, para ahorrar batería.

Las etiquetas pasivas funcionan sin una batería interna, obteniendo la potencia que necesitan para funcionar del campo generado por el interrogador.
La ausencia de batería provoca que los transpondedores pasivos sean mucho más ligeros, pequeños, flexibles y baratos que los activos, hecho que redunda en que puedan ser diseñados en una amplia gama de formas. Además, ofrecen un tiempo de vida prácticamente ilimitado.

Como contrapartida, poseen unos radios de cobertura menores y requieren más cantidad de energía procedente del interrogador para poder transmitir los datos. También poseen restricciones a la hora de almacenar los datos y no funcionan demasiado bien en ambientes con interferencias electromagnéticas. Asimismo, su sensibilidad y orientación están limitadas por la potencia disponible.
Sin embargo, a pesar de estas limitaciones, las etiquetas pasivas ofrecen mejores ventajas en términos de costo y longevidad.

Existe un tipo especial de etiqueta pasiva que sí incorpora una batería, pero la misión de ésta es alimentar la circuitería interna del microchip. Nunca se utiliza esa energía para transmitir.
Resumimos la comparativa de las principales características en la siguiente tabla.

	Etiquetas Activas	Etiquetas Pasivas
Incorporan Batería	Sí	No
Costo	Mayor	Menor
Tiempo de Vida	Limitado	Casi Ilimitado
Cobertura	Mayor	Menor
Capacidad de Datos	Mayor	Menor

Tabla 2.2. Etiquetas activas vs Etiquetas activas.

Tipo y Capacidad de los Datos Almacenados

Los datos almacenados en las etiquetas requieren algún tipo de organización, como por ejemplo identificadores para los datos o bits de detección de errores (bits de paridad, bits de redundancia cíclica), con el fin de satisfacer las necesidades de recuperación de datos. Este proceso se suele conocer como codificación de fuente.

La cantidad de datos que se desea almacenar, evidentemente dependerá del tipo de aplicación que se desee desarrollar. Básicamente, las etiquetas pueden usarse con el fin de transportar:

- *Un identificador*. El tag almacena una cadena numérica o alfanumérica que puede representar:

- *Una identidad*. Tanto para identificar un artículo de fabricación o un producto en tránsito, como para proporcionar una identidad a un objeto, un animal o un individuo.
- *Una clave de acceso* a otra información que se encuentra almacenada en un ordenador o sistema de información.

- *Ficheros de datos*. Se denominan PDF (*Portable Data Files*) y permiten el almacenamiento de información organizada, sin perjuicio de que adicionalmente exista un enlace a información adicional contenida en otro sitio. El objeto del PDF puede ser:

- Transmitir la información
- Iniciar Acciones

En términos de capacidades de datos son habituales los tags que permiten almacenar desde un único bit hasta centenares de kilobits, aunque ya hay prototipos en el orden del Mbit. Considerando que 8 bits representan un carácter, una capacidad de 1 kilobit permite almacenar 128 caracteres [7]
Los dispositivos de un único bit poseen dos estados: “la etiqueta está en zona de lector” o
“la etiqueta no está en la zona del lector”. Algunos permiten la opción de desactivar y activar el dispositivo. Estos transpondedores no necesitan un microchip, por lo que su costo de fabricación resulta muy barato [8]

Su principal área de aplicación se da en el campo de los dispositivos antirrobo, en particular en aplicaciones EAS (*Electronic Article Surveillance*), con propósitos de vigilancia electrónica de artículos de venta. El bit permite disparar una alarma cuando la etiqueta atraviesa el campo de acción del interrogador. Por otro lado, este tipo de etiquetas también suele utilizarse en aplicaciones de recuento de objetos o individuos.

Los dispositivos que permiten almacenar hasta 128 bits suelen portan un número de serie o de identificación junto con, normalmente, bits de paridad. Tales dispositivos pueden ser programados por el usuario.

Las etiquetas con capacidades de hasta 512 bits son siempre programables por el usuario e ideales para alojar identificadores y otros datos específicos, como números de serie, contenido de paquetes, instrucciones de los procesos a realizar o posiblemente resultados de anteriores transferencias interrogador-transpondedor.

Las etiquetas que permiten albergar 64 kilobits o más son portadoras de ficheros de datos.
Incrementando la capacidad, el servicio puede también permitir la organización de los datos en campos o páginas que pueden ser selectivamente interrogadas durante el proceso de lectura [9]

Velocidad de Lectura de Datos

La velocidad de lectura de los datos depende principalmente de la frecuencia portadora. En términos generales, cuanta más alta sea dicha frecuencia, más alta será la velocidad de transferencia.

Un aspecto a considerar es la velocidad con que las etiquetas se mueven dentro de la zona de lectura. El tiempo que tarda una etiqueta en atravesar una zona de lectura debe ser superior al tiempo de lectura de la propia etiqueta, o no dará tiempo al lector para que pueda realizar

adecuadamente la lectura. Este problema puede agravarse si son varias las etiquetas que el interrogador debe detectar, ya que cuando varios tags intentan transmitir sus datos a un mismo lector, el tiempo de lectura se multiplica por el número de tags.

Para etiquetas que poseen una alta capacidad de almacenamiento de datos, cuando se trata de leer toda la información almacenada en la etiqueta los tiempos de lectura serán en consecuencia elevados. En este sentido, la opción que poseen algunas etiquetas para realizar lecturas selectivas, por bloques o por sectores, puede ser muy beneficiosa para reducir considerablemente el tiempo de lectura.

A baja frecuencia (<135KHz) una unidad lectora estándar tardará aproximadamente 0.012 segundos en capturar la información de una etiqueta, permitiendo una velocidad de 3 m/s. Para velocidades más rápidas se necesitarían antenas más grandes. Por ejemplo ha sido posible realizar lecturas cuando las etiquetas se movían velocidades de 65 m/s (unos 240 km/h).

Opciones de Programación

Dependiendo del tipo de memoria que incorpore el transpondedor, los datos transportados pueden ser:

- *De sólo lectura*. Son dispositivos de baja capacidad, programados por el fabricante desde el primer momento. Normalmente portan un número de identificación o una clave a una base de datos donde existe información dinámica relativa al objeto, animal o persona a la que van adheridos.

- *De una escritura y múltiples lecturas*. Son dispositivos programables por el usuario, pero una única vez.

-*De lectura y escritura*. También son programables por el usuario pero adicionalmente permiten modificar los datos almacenados en la etiqueta. Los programadores permiten la escritura directamente sobre la etiqueta adherida al objeto en cuestión, siempre y cuando se encuentre dentro del área de cobertura del programador.

EPCGlobal, organización de empresas específicamente orientada a desarrollar estándares globales para un Código Electrónico de Producto (EPC, Electronic Product Code), tiene el objetivo de normalizar la información contenida en las etiquetas RFID. En la Tabla 2.3 se resumen los diferentes protocolos que especifica EPC junto con el tipo de etiquetas y rango de frecuencias que lleva asociadas.

Protocolo	Frecuencia	Tipo de Etiqueta
Clase 0	UHF	Sólo Lectura
Clase 0 Plus	UHF	Lectura-Escritura
Clase 1	HF / UHF	Una escritura – Múltiples lecturas
Clase 1 Generación 2	UHF	Una escritura – Múltiples lecturas
Clase 2	UHF	Lectura y Escritura

Tabla 2.3. Protocolos EPCGlobal para RFID

Cabe destacar que estas especificaciones se refieren al nivel físico (interfaz radio que permita leer la información en cualquier lugar del mundo) y de codificación (Código Electrónico del Producto unívoco). Aún está bajo desarrollo el interfaz ser servicios de información: EPC-IS (EPC Information Services) que permitirá la automatización de las cadenas de suministro de las empresas.

Forma física

Las etiquetas RFID pueden tener muy diversas formas, tamaños y carcasas protectoras, dependiendo de la utilidad para la que son creados. El proceso básico de ensamblado consiste en la colocación, sobre un material que actúa como base (papel, PVC), de una antena hecha con materiales conductivos como la plata, el aluminio o el cobre.
Posteriormente se conecta el microchip a la antena y opcionalmente se protege el conjunto con un material que le permita resistir condiciones físicas adversas. Este material puede ser PVC, resina o papel adhesivo. [10]

Una vez construida la etiqueta, su encapsulación puede variar de modo que faciliten su inserción o acoplamiento a cualquier material (madera, plástico, piel, etc).

Con respecto al tamaño, es posible desarrollar etiquetas del orden de milímetros hasta unos pocos centímetros. Por ejemplo los transpondedores empleados en la identificación de ganado, que son insertados bajo la piel del animal, miden entre 11 y 34 mm, mientras que aquellos que se encapsulan en discos o monedas, suelen tener un diámetro de entre 3 y 5 cm. Las etiquetas inteligentes RFID tienen las medidas estandarizadas de 85.72 mm x 54.03 mm x 0.76 mm ± tolerancias.

Algunas de las formas que pueden albergar un transpondedor pueden agruparse en:

- Transpondedores encapsulados en ampollas, monedas, pilas, llaves, relojes, varillas, cápsulas, discos, botones. La figura que sigue da una idea de la amplia variedad de formas que existen.

- Etiquetas inteligentes: pueden ser tarjetas o tickets, que tienen el mismo formato que las habituales tarjetas de crédito, a las que se le incorpora un tag RFID impreso. Esto permite la utilización de la tarjeta tradicional sin necesidad de contacto físico con un lector.

Costos

Las principales variables que influyen en el costo de las etiquetas son el tipo y cantidad que se adquieran. Respecto a la cantidad, la relación está clara: cuantas más etiquetas se compren, menor será su precio.

En relación al tipo de etiquetas, se pueden considerar los siguientes factores:

- *La complejidad de la lógica del circuito*, de la construcción de la etiqueta o de su capacidad de memoria, influirá en el costo tanto de los transpondedores como de los lectores y programadores.
- *La forma de la etiqueta*, es decir, el modo en que el dispositivo es encapsulado para formar la etiqueta. Algunas aplicaciones pueden requerir carcasas robustas mecánica o químicamente, o de alta tolerancia a las variaciones de la temperatura, debido a las condiciones de trabajo a las que deben funcionar. El encapsulado en dichas circunstancias puede representar una proporción significativa del costo total del transpondedor (el 30%).
- *La frecuencia de trabajo de la etiqueta*. En general, los transpondedores de baja frecuencia son más baratos que los de alta frecuencia.
- *El tipo de etiqueta*: posibilidades de lectura/escritura, activas o pasivas. Los tags pasivos son más baratos que los activos.

Para grandes cantidades de etiquetas, el precio puede variar entre unos pocos céntimos, para etiquetas muy simples hasta decenas de dolares para dispositivos más sofisticados.

El precio objetivo actualmente es de 5 céntimos de euro por etiqueta, pero cómo lograrlo implica un amplio debate, ya que el camino para alcanzarlo seguramente implicará reducir las actuales capacidades que se esperan de la etiqueta.

2.2.4.2 Lectores

Un lector o interrogador es el dispositivo que proporciona energía a las etiquetas, lee los datos que le llegan de vuelta y los envía al sistema de información. Asimismo, también gestiona la secuencia de comunicaciones con el lector. A continuación se listan las funciones específicas que tiene el lector RFID:

• Suministra energía a las etiquetas pasivas, para comunicarse con ellas.
• Realiza anticolisión, filtrado y funciones de manejo del lector.

• Sirve de interfaz entre la etiqueta, el sistema de almacenamiento y el procesamiento de la información.
• Actúa con comandos del software de aplicación.
• Interroga a las etiquetas y colecta información de las memorias de las mismas.
• Convierten las ondas analógicas de radio en datos digitales.
• Almacenan y/o transmiten datos a otros dispositivos con conexiones alámbricas o inalámbricas.
• Usualmente soportan múltiples protocolos (EPC, ISO).

Con el fin de cumplir tales funciones, está equipado con un módulo de radiofrecuencia (transmisor y receptor), una unidad de control y una antena. Además, el lector incorpora un interfaz a un PC, *host* o controlador, a través de un enlace local o remoto: RS232, RS485, Ethernet, WLAN (RF, WiFi, Bluetooth, etc.), que permite enviar los datos del transpondedor al sistema de información.

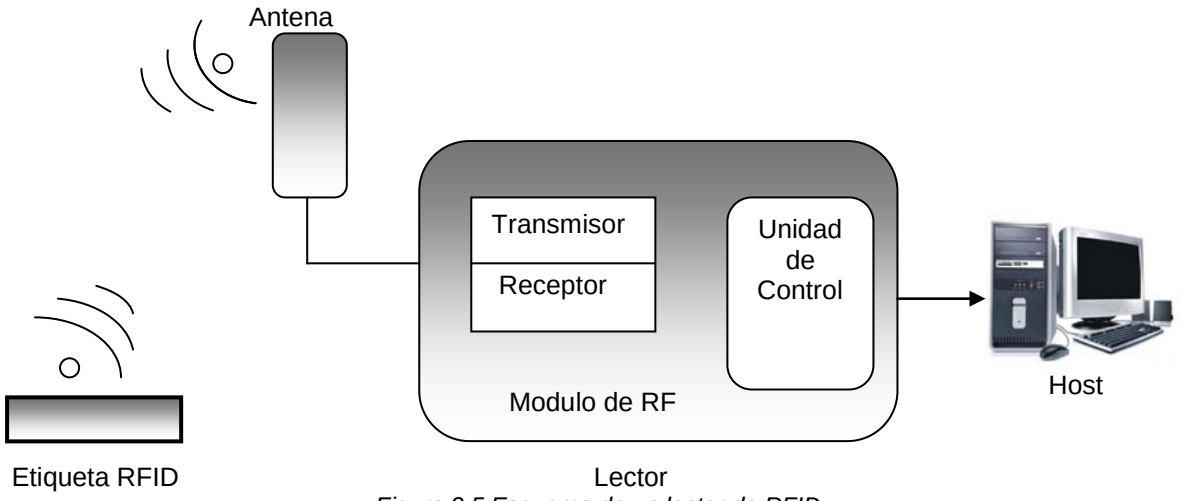


Figura 2.5 Esquema de un lector de RFID.

El lector puede actuar de tres modos:

Interrogando su zona de cobertura continuamente, si se espera la presencia de múltiples etiquetas pasando de forma continua.

- Interrogando periódicamente, para detectar nuevas presencias de etiquetas.
- Interrogando de forma puntual, por ejemplo cuando un sensor detecte la presencia de una nueva etiqueta.

Los componentes del lector son, como podemos ver en la Figura 2.8, el módulo de radiofrecuencia (formado por receptor y transmisor), la unidad de control y la antena. A continuación se procede a describir un poco más cada uno de estos elementos.

- El módulo de radiofrecuencia, que consta básicamente de un transmisor que genera la señal de radiofrecuencia y un receptor que recibe, también vía radiofrecuencia, los datos enviados por las etiquetas. Sus funciones por tanto son:

- Generar la señal de radiofrecuencia para activar el transpondedor y proporcionarle energía.
- Modular la transmisión de la señal para enviar los datos al transponedor.
- Recibir y demodular las señales enviadas por el transponedor.

- La unidad de control, constituida básicamente por un microprocesador. En ocasiones, para aliviar al microprocesador de determinados cálculos, la unidad de control incorpora un circuito integrado ASIC (*Application Specific Integrated Circuit*), adaptado a los requerimientos deseados para la aplicación.

  La unidad de control se encarga de realizar las siguientes funciones:

- Codificar y decodificar los datos procedentes de los transpondedores.
- Verificar la integridad de los datos y almacenarlos.
- Gestionar el acceso al medio: activar las etiquetas, inicializar la sesión, autenticar y autorizar la transmisión, detectar y corregir errores, gestionar el proceso de multilectura (anticolisión), cifrar y descifrar los datos, etc.
- Comunicarse con el sistema de información, ejecutando las órdenes recibidas y transmitiéndole la información obtenida de las etiquetas.

  Una de las funciones más críticas que debe realizar la unidad de control es gestionar el acceso al medio. Cuando se transmite información mediante una tecnología que no requiere contacto físico, existe la posibilidad de que aparezcan interferencias que provoquen cambios indeseados a los datos transmitidos y, en consecuencia, errores durante la transmisión. Para evitar este problema se utilizan procedimientos de comprobación (checksum). Los más comunes son la comprobación de bits de paridad, comprobación de redundancia longitudinal (LRC, Longitudinal Redundancy Check) y comprobación de redundancia cíclica (CRC, Cyclic Redundancy Check).

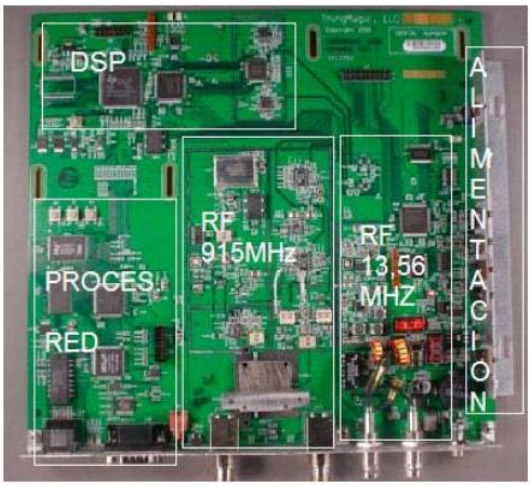


Figura 2.6 Diseño interno de un lector que puede trabajar con dos frecuencias.

El número de etiquetas que un lector puede identificar en un instante de tiempo depende de la frecuencia de trabajo y del protocolo utilizado. Por ejemplo, en la banda de Alta Frecuencia suele ser de 50 tags por segundo, mientras que en la banda de Ultra Alta Frecuencia puede alcanzar las 200 tags por segundo.

- La antena del lector es el elemento que habilita la comunicación entre el lector y el transpondedor. Las antenas están disponibles en una gran variedad de formas y tamaños. Su diseño puede llegar a ser crítico, dependiendo del tipo de aplicación para la que se desarrolle. Este diseño puede variar desde pequeños dispositivos de mano hasta grandes antenas independientes. Por ejemplo, las antenas pueden montarse en el marco de puertas de acceso para controlar el personal que pasa, o sobre una cabina de peaje para monitorizar el tráfico que circula.

La mayor parte de las antenas se engloban en alguna de las siguientes categorías:

- Antenas de puerta (uso ortogonal).
- Antenas polarizadas circularmente.
- Antenas polarizadas linealmente.
- Antenas omnidireccionales.
- Antenas de varilla.
- Dipolos o múltipolos.
- Antenas adáptativas o de arrays.

Figura 2.7 Distintos tipos de antenas de baja frecuencia. De pie: antenas de puerta; en el suelo: antenas de varilla.

El elemento más característico de la antena del lector es la frecuencia de operación a la que trabaja el sistema. Sin embargo, existen otra serie de parámetros físicos que es necesario considerar: impedancia, máxima potencia permitida, ganancia, patrón de polarización (polarización X-Y o circular). Estos son los elementos clave que crean el campo de radiofrecuencia, pero a su vez están influenciados por otros parámetros, como la eficiencia de la antena o el tipo de acoplamiento con la antena de la etiqueta. En general, las posibilidades que brinda el tipo de antena, su conexión al lector y su ubicación son innumerables. Cabe destacar que algunos lectores (principalmente aquellos que trabajan en campo cercano, como los lectores de mano), incorporan la antena integrada en el lector, lo que reduce enormemente esta flexibilidad.

El principal aspecto a considerar a la hora de elegir una antena, es el área de cobertura requerido para la aplicación, de modo que sea lo suficientemente grande para detectar las etiquetas pero lo suficientemente pequeño para evitar lecturas espurias no válidas que pueden afectar y confundir al sistema.

Otro aspecto que puede afectar a la cobertura es la orientación de la antena del lector con respecto a la etiqueta, que influye sobre la cantidad de potencia transferida al tag, afectando en ocasiones de forma significativa a la lectura.
A pesar de que las etiquetas pueden leerse en todas las orientaciones, en general el campo generado por la antena del lector tiene una dirección determinada. Este hecho influye especialmente en AF y UHF, pudiendo reducirse la cobertura al 50% o incluso imposibilitando la lectura de la etiqueta. Por ello, resulta conveniente buscar el acoplamiento óptimo entre ambas antenas, y si la orientación de la etiqueta no puede controlarse se debe buscar una compensación mediante un adecuado diseño de la antena. [11]

Todos estos aspectos hay que tenerlos en cuenta antes de adquirir el lector, ya que en general todas las antenas RFID se presentan como productos finales, por lo que es necesario analizar previamente sus características. Sin embargo, la mayoría son sintonizables de modo que puedan ajustarse a la frecuencia de operación seleccionada para el sistema. Esto las hace susceptibles a multitud de factores externos, como son:

- Variaciones RF.
- Pérdidas por proximidad de metales.
- Variaciones del entorno.
- Efectos armónicos.
- Interferencias con otras fuentes de RF.
- Reflexiones de la señal.
- Diafonía (cross-talk)

El problema de desintonización de la antena, como consecuencia del efecto de estos factores, puede corregirse mediante la introducción de circuitos dinámicos auto sintonizadores, que realimentan continuamente la antena para que ésta esté siempre bien sintonizada.

Una vez que una etiqueta es detectada y seleccionada, el lector puede realizar operaciones sobre ella, es decir, leer su información o escribir en ella. Después de finalizar la operación, el lector descarta la etiqueta para proceder a interrogar a la siguiente. Existen algoritmos como el “Protocolo Orden-Respuesta”, en el que el lector ordena a un transpondedor que cese su transmisión, cuando reconoce que ya ha recibido la información. Otro método alternativo, más seguro pero más lento y costoso, se denomina “Sondeo Selectivo”, donde el lector busca específicamente las etiquetas que tienen una determinada identificación y las interroga por turnos. Por último, otra aproximación, aunque más cara, incluye el empleo de varios lectores multiplexados en único interrogador [12].

Los lectores pueden variar su complejidad considerablemente dependiendo del tipo de transpondedor que tengan que alimentar y de las funciones que deban desarrollar. Una posible clasificación los divide en fijos o móviles dependiendo de la aplicación que se considere.

- Los dispositivos fijos se posicionan en lugares estratégicos como puertas de acceso, lugares de paso o puntos críticos dentro de una cadena de ensamblaje, de modo que puedan monitorizar las etiquetas de la aplicación en cuestión.

Figura 2.8 Lector RFID fijo.

- Los lectores móviles suelen ser dispositivos de mano. Incorporan una pantalla LCD, en teclado para introducir datos y una antena integrada dentro de una unidad portátil. Por esta razón, su radio de cobertura suele ser menor.

Figura 2.9 Lectores RFID de mano

Los principales parámetros que caracterizan un lector RFID son:

- *Frecuencia de operación*. El lector puede funcionar a baja frecuencia, alta frecuencia, ultra alta frecuencia y frecuencia de microondas. Ya existen en el mercado lectores multi frecuencia.

- *Protocolo de funcionamiento*. Muchas compañías ofrecen soporte multiprotocolo (ISO, propietarios, etc), pero no admiten todos los protocolos existentes.

- *Tipo de regulación que siguen*. Por ejemplo, existen distintas regulaciones de frecuencia y de potencia en Estados Unidos y en Europa:
  - La banda de UHF funciona a 902 – 930 MHz en Estados Unidos y a 869 MHz en Europa.
  - La máxima potencia permitida es de 2 Watios en Estados Unidos y 0.5 Watios en Europa.

- *Interfaz con el sistema host*:

  - TCP/IP.
  - WLAN.
  - Ethernet (10BaseT).
  - Serie: RS 232, RS 485.

- *Capacidad para multiplexar muchos lectores*:

  - A través de concentradores.
  - A través de middleware.

- *Capacidad para actualizar el software del lector on-line*:

  - Vía Internet.
  - Vía interfaz con el host.

- *Capacidad para gestionar múltiples antenas*, típicamente 4 antenas/lector.
- *Capacidad para interactuar con otros productos de* middleware.
- *Entrada/salida digital* para conectar otros dispositivos tales como sensores externos

  - Circuitos de control adicionales.

Modo de operación

Un lector RFID utiliza ondas de radio para leer la información almacenada en la etiqueta. Existen dos modos de interacción entre el lector y la etiqueta: En el primer modo el lector envía a la etiqueta la orden de transmitir la información que tiene almacenada, en el segundo modo la etiqueta transmite la información que contiene periódicamente, en espera de que algún lector la detecte.

Un lector puede utilizarse también para reescribir sobre una etiqueta, siempre y cuando el lector esté habilitado para ello y la etiqueta tenga esa capacidad.

2.2.4.3 Antenas

La antena se encuentra en la parte interna del Tag y es la que permite al chip transmitir la información de identificación a un lector que convierte las ondas de radio reflejadas
Por la etiqueta en información digital que se puede procesarse mediante sistemas de computo.

Las antenas RFID usadas en sistemas de recolección de datos, en su mayoría caen dentro de las siguientes categorías: antenas tipo cuadro, con núcleo de ferrita, polarizadas circulares y lineales, omni direccionales, antenas di-polo o multi-polo.

Las antenas tipo “cuadro” son similares a las usadas en los almacenes para evitar robos, las cuales al tener mayor tamaño pueden alcanzar distancias de lectura del orden de un metro, aunque con poca direccionabilidad.

Las antenas con núcleo de ferrita tienen un tamaño más reducido por lo que su rango se disminuye a unos pocos centímetros. Sin embargo su menor tamaño permite su uso en equipos portátiles. Además son más direccionales, por lo que se pueden leer etiquetas que estén próximas entre sí [13].

2.2.4.4 Programadores

Los programadores son los dispositivos que permiten escribir información sobre la etiqueta RFID. La programación se realiza una vez sobre las etiquetas de sólo lectura o varias veces si las etiquetas son de lectura/escritura. Es un proceso que generalmente se suele llevar a cabo “fuera de línea”, es decir, antes de que el producto entre en las distintas fases de fabricación.

El radio de cobertura al que un programador puede operar, es generalmente menor que el rango propio de un lector, ya que la potencia necesaria para escribir es mayor. En ocasiones puede ser necesario distancias próximas al contacto directo.
Por otro lado, el diseño de los programadores permite una única escritura cada vez. Esto puede resultar engorroso cuando se requiere escribir la misma información en múltiples etiquetas. Sin embargo, nuevos desarrollos de programadores vienen a satisfacer la necesidad de realizar la programación de múltiples etiquetas.
Existen sistemas en los que la reprogramación puede desarrollarse “en línea”, es decir, permaneciendo la etiqueta sobre el articulo cuya información o identificación porta. Esto resulta especialmente interesante si se trata de un fichero de datos interactivo, que va cambiando dentro de un proceso de producción. De este modo, los datos pueden irse modificando según el artículo vaya pasando por las distintas etapas de producción. El hecho de quitar la etiqueta del artículo para poder escribir la nueva información reduciría en gran medida las ventajas de flexibilidad inherentes a la tecnología RFID [14].
La combinación de las funciones de un lector/interrogador con las de un programador permite recuperar y modificar los datos que porta el transpondedor en cualquier momento, sin comprometer la línea de producción.

Un tipo especial de programador es la impresora RFID. Existen impresoras con capacidad de lectura/escritura, que permiten programar las etiquetas a la vez que se imprime con tinta información visible. Antes de realizar la escritura de la etiqueta, deben introducirse los datos deseados en la impresora. Una vez escritos, un lector a la salida comprueba la fiabilidad de los datos. Evidentemente este tipo de programación debe realizarse sobre etiquetas especiales hechas de materiales flexibles y que permiten la impresión en su exterior.

Figura 2.10 Ejemplo de Impresora RFID Printronix.

2.2.4.5 Middleware

El middleware es el software que se ocupa de la conexión entre el hardware de RFID y los sistemas de información existentes (y posiblemente anteriores a la implantación de RFID) en la empresa. Del mismo modo que un PC, los sistemas RFID hardware serían inútiles sin un software que los permita funcionar. Esto es precisamente el middleware. Se ocupa, entre otras cosas, del encaminamiento de los datos entre los lectores y etiquetas y los sistemas de información de la empresa, y es el responsable de la calidad y usabilidad de las aplicaciones basadas en RFID.

El middleware de RFID se ocupa de la transmisión de los datos entre los extremos de la transacción. Por ejemplo, en un sistema RFID basado en etiquetas, en el proceso de lectura se ocuparía de la transmisión de los datos almacenados en una de las etiquetas al sistema de información de la empresa. Las cuatro funciones principales del middleware de RFID son:

- *Adquisición de datos*. El middleware es responsable de la extracción, agrupación y filtrado de los datos procedentes de múltiples lectores RFID en un sistema complejo. Sin la existencia del middleware, los sistemas de información de las empresas se colapsarían con rapidez. Por ejemplo, se ha estimado que cuando Walmart empezó a utilizar RFID, generaba del orden de 2 TBytes de datos por segundo.

- *Encaminamiento de los datos*. El middleware facilita la integración de las redes de elementos y sistemas RFID en los sistemas de la empresa. Para ello dirige los datos al sistema apropiado dentro de la organización empresarial.
- *Gestión de procesos*. El middleware se puede utilizar para disparar eventos en función de las reglas de la organización empresarial donde opera, por ejemplo, envíos no autorizados, bajadas o pérdidas de stock, etc.
- *Gestión de dispositivos*. El middleware se ocupa también de monitorizar y coordinar los lectores RFID, así como de verificar su estado y operatividad, y posibilita su gestión remota.

Muchos de los middleware desarrollados o en desarrollo se ajustan a los estándares de EPCglobal, conocidos como Savant. La especificación Savant ordena los componentes del middleware de acuerdo a sus funciones.

En la actualidad, el desarrollo del middleware dista de ser algo acabado. Los sistemas actuales se centran sobre todo en la integración y la coordinación, con funciones de filtrado básicas. La evolución será hacia la gestión avanzada de dispositivos, integración de aplicaciones, integración de partners, gestión de procesos y posibilidad de desarrollo de aplicaciones.

Debido al reciente interés que ha surgido en el middleware, han aparecido gran cantidad de suministradores, aunque no se puede decir que en la actualidad exista ninguno que sea dominante. Algunos de los actores en el mercado en este momento son:

- Proveedores de software de aplicación empresarial, que ofrecen adiciones RFID a las aplicaciones de software empresarial existentes.
- Proveedores de software de infraestructura, como Sun, IBM, Oracle, SAP, y Microsoft, que están ampliando sus productos middleware existentes para incluir la RFID.
- Los fabricantes de equipamiento RFID extienden sus líneas de producto y se introducen en el mercado del middleware. Como ejemplos tenemos Zebra, Check Point e Internec.

El software RFID debe ser capaz de administrar la interacción entre el lector, las etiquetas y la aplicación para el usuario. Para realizar estas actividades el software RFID ha sido dividido en 3 capas las cuales se ilustran en la figura 2.11, y se detallan a continuación:

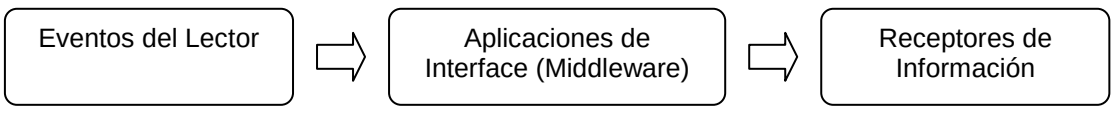


Figura 2.11 Arquitectura del software RFID. Fuente: Elaboración Propia

- Eventos de lector: Esta capa controla el intercambio de información entre el lector y las etiquetas RFID, por lo que se encarga de realizar las siguientes funciones:

• ***Lectura y Escritura***: Estas son las funciones más básicas de una etiqueta RFID. La lectura ocurre cuando la etiqueta está en el rango de transmisión del lector y éste accede a la información que la memoria de la etiqueta contiene; la escritura en la etiqueta sucede cuando el usuario reescribe la memoria de la etiqueta a través del lector usando la aplicación del usuario.

• ***Anticolisión:*** Esta función está presente en sistemas especiales en los cuales el lector puede identificar varias etiquetas al mismo tiempo (habitualmente las etiquetas deben entrar una a una en la zona de cobertura del lector).

• ***Detección y corrección de errores:*** Esta función la realiza el lector, el cual debe ser capaz de detectar y descartar información incompleta o duplicada.

• ***Seguridad****:* La seguridad de un sistema RFID se refiere a la encripción de la información, la autorización y autenticación entre los dispositivos RFID para evitar que lectores desconocidos capten la información de las etiquetas, cabe aclarar que incorporar estas funciones en un sistema RFID encarece el costo de las etiquetas.

- Aplicaciones de interface: Esta capa opera entre los lectores y las aplicaciones del usuario, realiza dos funciones importantes las cuales son:

• ***Manejo de flujo de datos entre lectores y las aplicaciones del usuario:*** Esta función se refiere al tratamiento que se le dará a la información que el lector recibe de las etiquetas; es decir permite traducir la información, filtrarla, asociarla a diferentes eventos mediante la aplicación del usuario y agregarla en la etiqueta si es que ésta posee dicha funcionalidad.

• **Operación de dispositivos RFID:** Esta función consiste en comandar el lector para leer y escribir las etiquetas, configurar los parámetros para la recepción y transmisión de los datos entre las etiquetas y entre el computador, y monitorear el estado del lector automáticamente.

- Receptores de Información: Esta capa recibe la información de la etiqueta procesada por la capa de aplicación de interfaz, la aplicación del usuario es un programa utilizado para el control de inventarios, control de asistencia o acceso de personal, la administración de un almacén comercial, etc. Este programa debe administrar una base de datos que contendrá información detallada del objeto a ser identificado.

2.2.4.6 Sistemas de Información

De manera similar a los códigos de barras estándar, las etiquetas RFID son simplemente un modo automatizado para proporcionar datos de entrada al sistema cliente. Sin embargo, las etiquetas

RFID son capaces de proporcionar también una salida automatizada del sistema hacia la etiqueta, permitiendo la actualización dinámica de los datos que ésta porta.

El sistema de información se comunica con el lector según el principio maestro-esclavo.
Esto quiere decir que todas las actividades realizadas por lector y transpondedores son iniciadas por la aplicación software. Cuando el lector recibe una orden de esta aplicación, establece una comunicación con los transpondedores, comunicación en la que a su vez el lector ejerce de maestro y los tags de esclavos.

El principal objetivo de la aplicación software es gestionar y tratar los datos recibidos por el lector. El sistema debe ser lo suficientemente robusto para poder manejar las múltiples lecturas que permiten realizar los sistemas RFID, coordinar tiempos y flujos de información, gestionar los distintos eventos, soportar las realimentaciones de los usuarios, introducir las actualizaciones del sistema cuando sea requerido e integrarlo con otros sistemas de información de la empresa. En todos los casos el sistema cliente necesitará modificaciones software para integrar los datos proporcionados por el lector y el programador. Sin la posibilidad de acceder a todas estas funcionalidades, el sistema RFID perderá en eficacia y no proporcionará el deseado retorno de la inversión.

Algunos de los sistemas de información de la empresa con los que se puede integrar un sistema RFID son: el sistema de planificación de recursos ERP (*Enterprise Resource Planning*), el sistema de gestión de almacenes WMS, (*Warehouse Management System*), el sistema de albaranes y comprobantes de entrega POD (*Proof Of Delivery*) o el sistema de comprobantes de recogida POC (*Proof Of Collection*).

2.2.5 Clasificación detallada de los sistemas RFID

Los sistemas RFID se pueden clasificar siguiendo varios criterios, como pueden ser la frecuencia a la que trabajan los sistemas (LF, HF, UHF o microondas), la alimentación de los transponders (activos o pasivos) o según el principio de funcionamiento en el que se basan (acoplamiento inductivo, backscatter o microwave) [15].

Como ya se ha hecho hincapié en estas diferencias, es conveniente centrarse en otras características que diferencian entre sí los sistemas de RFID. Estas clasificaciones tienen por criterio diferencial el sistema de memoria que incorpora el transponder, el rango de información y la capacidad de procesamiento que tiene el transponder o el procedimiento de comunicación que se realiza entre transponder y lector.

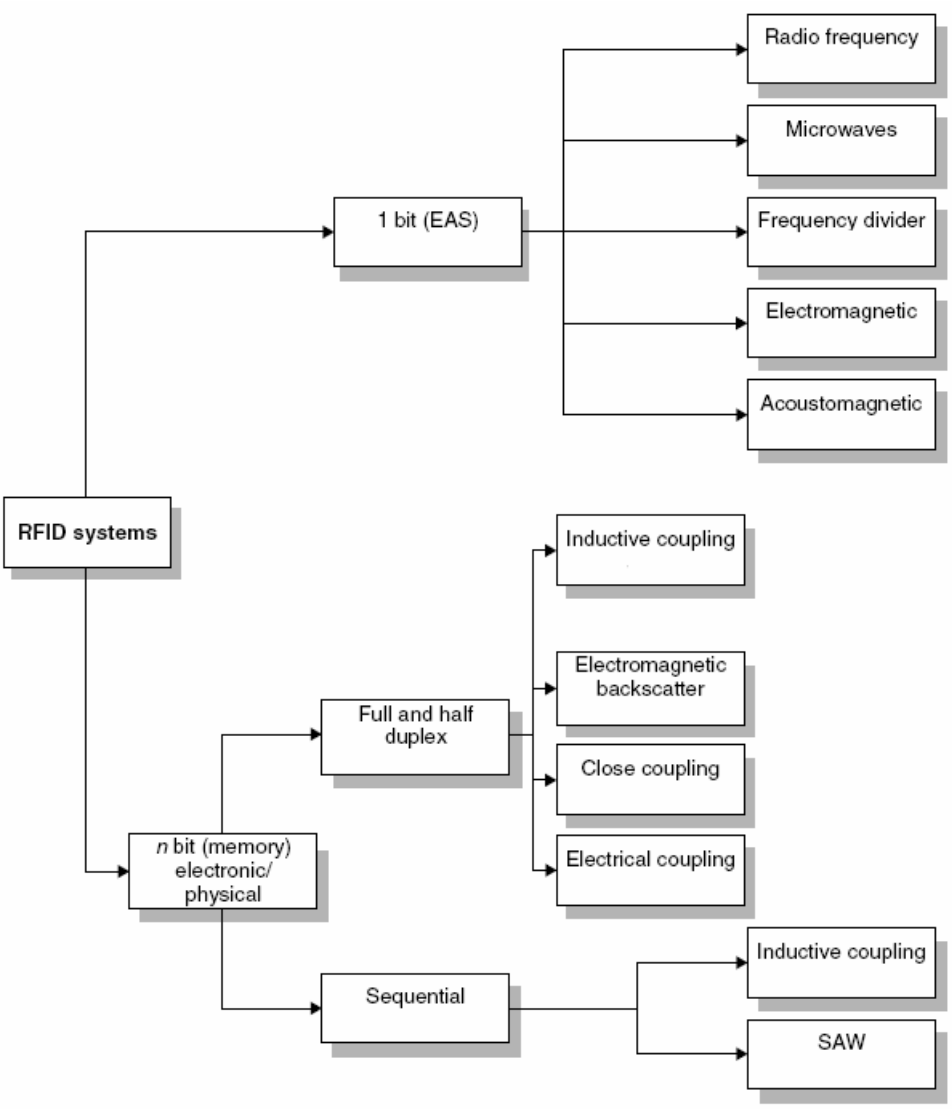


Figura 2.12 Esquema de los diferentes principios de operación de los sistemas RFID.

Uno de estos criterios es según el rango de información y la capacidad de proceso de datos que ofrece el transponder, así como el tamaño de su memoria de datos. Realizando esta clasificación obtenemos un amplio espectro de variantes que se dividen en sistemas Low-end, Mid-range y High-end [16].

- Sistemas Low-end: los sistemas EAS (Electronic Article Surveillance) componen principalmente este grupo, son sistemas que reconocen la presencia de un artículo en la zona de alcance del lector. Transponders de sólo lectura también son sistemas Low-end, estos transponders tienen grabados permanentemente los datos que pueden consistir en un único número de serie. Si una de estas etiquetas entra en el radio de acción de un lector inicia una comunicación broadcast con su número de serie. Existe el problema de que haya la presencia de más de un transponder en el radio de acción del lector, en este

caso puede haber una colisión de datos enviados por los transponders y el lector no podrá detectar ninguno de ellos. Estos sistemas son adecuados para diversas aplicaciones que necesitan cantidades de información pequeñas. Por ejemplo sustituyendo a los códigos de barras, ya que la simplicidad de sus funciones permite que el área de chip sea reducida, así como su consumo y su costo de producción. Estos sistemas son capaces de trabajar en todo el rango de frecuencias que opera RFID.

- Sistemas Mid-range: estos sistemas permiten la escritura en la memoria. El tamaño de la memoria va desde los pocos bytes hasta el orden de 100Kbyte EEPROM (transponders pasivos) o SRAM (transponders activos). Estos transponders son capaces de procesar comandos simples de lectura para la selectiva lectura/escritura de la memoria en una máquina de estados permanentemente codificados. Estos transponders son capaces de soportar procesos de anticolisión, por lo que varios transponders en el radio de acción de un lector no se interfieren y el lector es capaz de diferenciarlas. En estos sistemas se utilizan procedimientos de encriptación de datos y autentificación entre lector y transponder. Estos sistemas son capaces de trabajar en todo el rango de frecuencias que opera RFID.

- Sistemas High-end: estos sistemas poseen microprocesadores y un sistema de funcionamiento de tarjeta inteligente. El uso de los microprocesadores facilita el uso de algoritmos de autentificación y encriptación más complejos. Estos sistemas operan en una frecuencia de 13.56 MHz.

Podemos clasificar los sistemas de RFID según la cantidad de información que contiene los transponders.

Aunque los sistemas RFID suelen tener una capacidad de información que va desde los pocos bytes a centenares de KBytes. Pero existen numerosos sistemas que únicamente poseen un bit de información, los justos para tener controlados dos estados por el lector: la presencia del transponder en el campo creado por el lector o la ausencia del transponder. A pesar de su simpleza, son sistemas especialmente adecuados para aplicaciones como monitorizaciones o funciones de señalización. Debido a que los “1- bit transponder” como son conocidos, no precisan un chip electrónico, su costo es ínfimo.

Una de sus principales aplicaciones es el EAS (Electronical Article Surveillance) para la protección de objetos en tiendas y negocios. Cuando alguien intenta sustraer un articulo, sin haber sido desactivado el transponder, debe pasar por un lector situado en la salida de la tienda, si el lector detecta la presencia de un transponder inicia la reacción apropiada.

Estos sistemas pueden clasificarse según también su principio de funcionamiento: procedimiento RF basado en unos circuitos LC o circuito resonante ajustados a una determinada frecuencia de resonancia; sistemas EAS en el rango de microondas que generan armónicos con componentes con características no lineales como los diodos; divisores de frecuencia que operan en el rango de 100-135,5 KHz donde la frecuencia de resonancia proporcionada por el lector es dividida en el transponder y enviada hacia el lector nuevamente, generalmente dividida entre 2.

Los denominados “Electromagnetic types” o tipos electrónicos que usan campos magnéticos muy fuertes en el rango NF (10Hz-20KHz), los elementos de seguridad contienen una línea metálica que sufren una saturación magnética ya que está sometida a un campo magnético muy fuerte y alternante, esto crea unos armónicos a la frecuencia básica del lector.

También es posible superponer frecuencias más elevadas a la señal básica; como son elementos no lineales crean frecuencias suma y diferencia con las frecuencias añadidas. El lector no reacciona a los armónicos de la frecuencia básica pero si que lo hace a la frecuencia suma o diferencia de las señales creadas.

Por último tenemos a los sistemas acústico magnético basados en pequeñas cajas de plástico que contienen dos líneas metálicas, una de ellas no esta conectada a la caja y produce una pequeña vibración al pasar por un campo magnético. La amplitud de esta vibración es especialmente alta si la frecuencia del campo magnético alterno producido por el lector, corresponde con la frecuencia de resonancia de la línea metálica.

Para contrastar con los transponders de un solo bit, el cual normalmente explota los efectos físicos (procesos oscilación estimulada, estimulación de armónicos por diodos no lineares en la curva de histéresis de metales), existen transponders que usan un microchip electrónico como sistemas portador de datos. Tienen una capacidad de almacenamiento de información mayor a pocos Kbytes. Para leer o escribir en estos sistemas de almacenamiento se realiza una transferencia de datos entre lector y transponder, esta transferencia puede seguir tres procesos: half duplex, full duplex y secuencial.

Podemos ver un esquema de la transmisión downlink y uplink de los tres procesos en la figura 2.13.

Dentro de la clasificación que podemos hacer por la cantidad de información transmitida, cuando hablamos de memorias con más de un bit podemos realizar otra clasificación a tenor del procedimiento que sigue la comunicación entre lector y etiqueta.

Sistemas half/full duplex: El lector inicia la comunicación con el transponder. El transponder responde en broadcast cuando detecta el campo RF.

Debido a que la señal generada por el transponder que recibe el lector es mucho más débil que la propia señal generada por el lector, éste debe tener sistemas capaces de diferenciar ambas

señales. En la práctica la transferencia de datos se realiza por modulaciones con portadora o subportadoras, pero también con armónicos de la frecuencia de transmisión del lector.

La diferencia radica en que en los sistemas half duplex la transferencia de datos entre lector y transponder, se alterna con la comunicación entre transponder y lector. Estos sistemas suelen usar las modulaciones de carga con o sin subportadora, y armónicos.

Por lo que se refiere a los sistemas full duplex, la comunicación entre el transponder y el lector se realiza al mismo tiempo que la comunicación entre lector y transponder. Incluye procedimientos en la que la transferencia de datos se realiza mediante en una fracción de frecuencia del lector, en subarmónicos o en frecuencias completamente distintas, no armónicos.

Estos sistemas utilizan como principios de funcionamiento para la transmisión y recepción de datos, el acoplamiento inductivo, backscatter, close coupling y electrical coupling.

Sistemas secuenciales: Emplean el sistema en el cual el campo generado por el lector se enciende y se apaga en intervalos regulares. Lo que significa que el transponder es alimentado de forma intermitente (pulso). La transferencia entre transponder y lector se produce en esos intervalos en los que el lector no se comunica con el transponder. La desventaja de estos sistemas es la pérdida de energía en el transponder en los intervalos que se corta la comunicación, este problema puedes ser solucionado con una alimentación externa.
Estos sistemas utilizan como principios de funcionamiento para la transmisión y recepción de datos, el acoplamiento inductivo y SAW (Surface Acoustic Wave); basado este último en el efecto piezoeléctrico y una dispersión en la superficie de las ondas acústicas a pequeña velocidad.

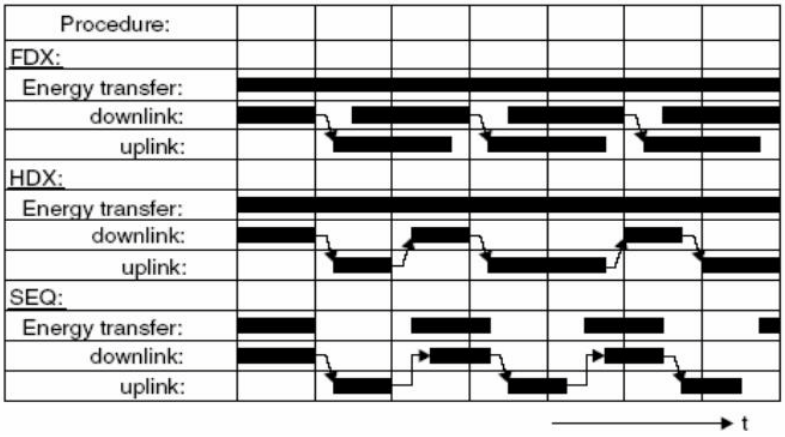


Figura 2.13 Esquema de los diferentes procedimientos, Full-duplex, Half-duplex y Secuencial.

Se puede clasificar los sistemas RFID según el tipo de memoria del transponder, EEPROM, FRAM o SRAM. Existen numerosos transponders que tienen únicamente con información de un número de serie que se incorpora cuando se fabrica y no puede ser alterado después. En otro tipo de transponders sí es posible el escribir en la memoria.

- EEPROM (Electrically Erasable Programmable Read-Only memory): la memoria más utilizada en acoplamiento inductivo. Como desventaja tiene el alto consumo de energía durante la operación de escritura y el número limitado de ciclos de escritura (100.000 y 1.000.000).

- FRAM (Ferromagnetic Random Access Memory): tiene un consumo del orden de 100 veces menor que los EEPROMs y el tiempo de escritura 1000 veces menor.

- SRAM (Static Random Access Memory): más utilizado en los sistemas de microondas. Facilita rápidamente el acceso a los ciclos de escritura. Por el contrario necesita un suministro de energía ininterrumpido de una batería auxiliable.

  En sistemas programables la lectura, escritura y la autorización se realizan mediante lógica interna. Mediante máquinas de estado generalmente, se pueden realizar secuencias complejas, pero no posibilita cambios en el programa sin realizar cambios en el layout. El uso de microprocesadores mejora este problema, incluyendo software para cada aplicación.

  Podemos clasificar también los sistemas RFID según los diferentes procedimientos para enviar datos desde el transponder al lector.

- Reflexión o backscatter: La frecuencia de la transmisión es la misma que la usada por el lector para comunicarse con el transponder.

- Load modulation: El campo del lector es influenciado por la frecuencia del transponder.

- Subarmónicos: Uso de subarmónicos (1/n) y la generación de ondas armónicas de frecuencia múltiplos de n en el transponder.

2.3 Mercado de RFID

El mercado actual del RFID está en una fase de crecimiento de crecimiento, pero cambia según la región a la que nos referimos. Si hablamos de EEUU, el RFID ha tenido un crecimiento muy elevado gracias a los mandatos, pero ahora se está sosteniendo gracias a los proyectos lanzados por las propias empresas para mejorar sus procesos al margen de estos mandatos.

El último análisis realizado por Frost & Sullivan[1] indica que en Asia-Pacifico el uso de la RFID ha

[1] Empresa consultora con sede en New York, fundada en 1975 tiene presencia en mas de 40 países y se encarga de proveer de datos estadísticos a empresas de cualquier ramo ya sea industria o servicios.

dejado una derrama económica de 170.3 millones de dólares en el 2006 y se cree que en 2013 se llegue a 646.3 millones de dólares.

En Europa, el mercado es similar puesto que es en aquel continente donde han surgido investigaciones sobresalientes que han complementado las bases y han hecho una pronta evolución satisfactoria de esta tecnología que ha sido adoptada por numerosas empresas y sectores gubernamentales. Prueba de ello son las cifras de Frost & Sullivan que indican que los ingresos por el uso de esta tecnología han alcanzado en 2007 la cifra de 41 millones de dólares y que en 2013 alcanzar los 181 millones.

Como bien se sabe, América Latina ha evolucionado sustancialmente en la adopción de nuevas tecnologías en la industria de la seguridad y en el campo de la RFID no es la excepción.

Frost & Sullivan (2006, Informe sobre Crecimiento del uso del RFID)[1] sostiene que México es uno de los países de la región más interesados en la tecnología. Pero existen países como Colombia, Chile, Guatemala, Venezuela y Uruguay que manifiestan también interés en esta tecnología ya con algunas implementaciones, especialmente en salud y logística sin embargo aun esta tecnología ha despegado como se preveía.

Cabe destacar que en febrero de este año Frost & Sullivan pronosticó que el mercado de RFID, de tarjetas de identificación electrónica de productos, llegará a facturar en 2008 los 1.2 millones de dólares, lo que significa un aumento del 30,9%, con respecto a lo facturado en 2007, cuando se terminó facturando $917.3 millones.

2.4 Campos de Uso

La identificación por radiofrecuencia trabaja bajo varios tipos de frecuencias y dependiendo de ellas se enfoca el uso que se la da a los tags, depende del RFID, si trabajamos con frecuencias de 125khz, o mifare se orientan más al control de acceso o control de activos, pero pensando siempre en distancias relativamente cortas. Si trabajamos con UHF, que son frecuencias de aprox. 900Mhz, se puede combinar con tags pasivos que dan como ocho metros de distancia, lo cual se hace ideal para el control de inventarios, unidades móviles, contenedores etc. Si utilizamos tags activos podemos controlar todo tipo de equipo electrónico, también se puede utilizar en personas vía pulseras especiales con las que se puede tener un rango de lectura de hasta 50m.

[1] Frost & Sullivan, (2007), Crecimiento del Uso de la tecnología en el Mercado Mundial, Consultado en Mayo de 2009 en http://www.frost.com/prod/servlet/report-homepage.pag?repid=M06B-01-00-00-00&ctxst=FcmCtx1&ctxht=FcmCtx2&ctxhl=FcmCtx3&ctxixpLink=FcmCtx4&ctxixpLabel=FcmCtx5

Los otros tipos de frecuencias también están difundidos en el mercado, como el de alta, 13,56 MHz, la cual no funciona cerca de los metales. Normalmente se utiliza en aplicaciones como la trazabilidad de los productos, movimientos de equipajes de avión o acceso a edificios. Por su parte, la frecuencia de microondas (2,45 GHz y 5,8 GHz), se utiliza para largas distancias de lectura, así como para altas velocidades de transmisión, y es usada para seguimiento y trazabilidad de personas u objetos.

El control de activos por radiofrecuencia puede ser implementado en industrias, empresas, comercio, gobierno, entre otros con el fin de proteger sus equipos, personas y locaciones, ya que no sólo se usan para el rastreo sino también, por ejemplo, para permitir o restringir el acceso.

En el gobierno este sistema es implementado para controlar activos, accesos e Identificación de vehículos y acceso de personas (tarjetas de proximidad). De igual manera, en el sector salud se utiliza para la identificación de los pacientes con el propósito de registras los consumos hospitalarios que estos realicen así como el registro de la medicación que este siendo aplicada en ese momento. También admite la identificación de los activos médicos que se encuentran en hospitales y centros médicos. Evita los costos por pérdida de tiempo de pacientes y personal del hospital, así como los costos de reposición de los equipos. Ya que alrededor de un 10 a 20% de los equipos que se encuentran en hospitales y centros médicos son hurtados o extraviados. En la industria textil, por su parte, se implementa para supervisar activos e inventarios.

Asimismo se implementa en la seguridad de personal especial, por ejemplo, hace unos años se desarrollan pruebas de identificación para personas que se encuentren en zonas de conflicto como personal de organizaciones humanitarias, Cruz Roja, militares, etc. o en ciudades con altos índices de secuestro.

Para la identificación de animales, esta tecnología se usa como herramienta de control y de registro en programas de crianza de ganado. Mientras que en las bibliotecas permite el control de colecciones de libros e inventarios, agilizando los procesos rutinarios, además de posibilitar un registro permanente sobre las existencias y uso de las colecciones.

En logística su uso es el convencional con el fin de realizar un seguimiento de los productos a lo largo de la cadena de suministros. Y en almacenes de cadena RFID permite que se controlen los artículos o mercancía, pero en este sector existen algunos cambios como explica Cesar, pues en ciertos países se vienen desarrollando pruebas de utilización de la tecnología de RFID junto con la tecnología EAS (Electronic Article Surveillance), en un dispositivo conocido como *tag* dual, el cual

sirve como dispositivo de tracking y como dispositivo de seguridad, que deberá ser desactivado en el momento de la compra para garantizar que efectivamente el producto si fue pagado.

2.5 Soluciones Apoyadas en esta Tecnología

Las tarjetas de acceso para empleados están migrando más allá de solo servir como un sistema de seguridad sino que están conformando un conjunto de soluciones integrales donde se conjuga la atención, tiempo y seguridad a transacciones no lucrativas.

La tecnología RFID en conjunto entrega un rango de lectura, memoria y versatilidad de programación para la integración de sistemas de control de acceso, seguridad, autorización y hasta compras.

Esta tecnología es ideal para corporaciones que manejen una planta de tamaño considerable, naves industriales, planteles de educación, hospitales y centros de salud, centros penitenciarios, donde esta solución provea una localización en todo momento de cualquier persona, integrando sistemas que manejen seguridad, autorización, transacción e información.

Para tomar la decisión de implementar un sistema de seguridad y control de acceso en RFID se debe contemplar el precio y en el desempeño principalmente. Los sistemas de 125Khz brindan un precio razonable pero no ofrecen las nuevas funcionalidades para soluciones de seguridad y control de acceso sofisticado. Las soluciones de 13.56 MHz ofrecen ambas partes, a un precio bastante razonable con los sistemas de control de acceso tradicionales.
Tanto el personal de seguridad como administradores de planteles escolares y hospitalarios siempre buscan instalar nuevos sistemas para la seguridad de sus edificaciones, las soluciones de 13.56 MHz ofrecen compatibilidad con los sistemas de seguridad actuales y además ofrecen una pequeña migración de este para así añadirle nuevas funcionalidades y aplicaciones. Las Inversiones en tarjetas y lectores ofrecen la lectura de datos de manera inalámbrica, memoria, capacidad de lectura/escritura y programación de la tarjeta, para así colocar todos los datos necesitados en aplicaciones que ayuden a satisfacer las necesidades informativas de la organización.

Asegurar una sola área de la organización no es verdaderamente confiable. Empleados que se mueven de un punto a otro, vendedores que vienen y van, sistemas incompatibles a lo largo de todas las instalaciones, todo esto crea una serie de riesgos que pueden ser controlados con una red única de seguridad.

La tecnología RFID, basada en los estándares de calidad ISO, es un componente clave para una implementación de una red de seguridad que a su vez reduce costos, incrementa recursos de personal, reduce “tiempos muertos”, provee mecanismos centralizados para gestionar información de primera mano.

Las soluciones RFID proveen un sistema de Identificación único, versatilidad de la información, lectores “manos libres” de altas velocidades para manejar grandes números de personas. RFID puede conectar rápidamente a sus usuarios con una Base de Datos de un sistema de seguridad, ofreciendo así, control de acceso seguro a ciertas locaciones. Esta tecnología se puede combinar además con sistemas biométricos y otras tecnologías de seguridad para alcanzar así altos niveles de control y seguridad.

Implementar un control de acceso que integre el personal de la organización y los vehículos que ingresan a esta, puede fortalecer un débil vinculo en las operaciones de seguridad de dicha organización. Las soluciones RFID pueden controlar la seguridad del estacionamiento y el control de acceso a las edificaciones, brindando así al personal una forma más sencilla de ingresar.

Desde entrar al estacionamiento, y hasta la seguridad dentro del edificio, un simple sistema RFID puede proveer toda la seguridad a lo largo de toda una organización.

A continuación se muestran algunos casos de éxito donde se ha optado por utilizar la tecnología RFID:

Estacionamiento de Hospital Gleneagle en Singapur

El Personal médico del Hospital Gleneagle[1] en Singapur está utilizando la tecnología RFID para minimizar los retrasos al momento de entrar o salir del estacionamiento y así eliminar posibles embotellamientos en las horas pico.

Los autos de los empleados están equipados en sus ventanas con un transmisor de baja frecuencia que puede ser leído por una puerta automática con un lector RFID a 1.8 metros de distancia. Antes que este sistema fuese implementado, los 1000 empleados del hospital tenían que esperar para que los registros de entrada/salida del estacionamiento fueran atendidos manualmente, lo cual obviamente generaba un embotellamiento en las puertas de entrada. Con el nuevo sistema RFID, la tasa de entrada al estacionamiento se duplicó y los porteros no son necesarios, haciendo que algunos costos de personal bajen un poco y la certeza de la información mejore. La seguridad también ha incrementado debido a que este sistema garantiza que los autos no autorizados no ingresen al hospital.

Además de controlar el acceso, el lector RFID recolecta información acerca de la frecuencia que un empleado utiliza el estacionamiento o cuánto tiempo dura un auto estacionado, y cuántos autos

[1] 286, Ground Floor, Gleneagle Hospital, Jln Ampang, 50450 Kuala Lumpur, Singapur

utilizan el estacionamiento en cada mes. Esta información es utilizada por el hospital para evaluar de una forma más efectiva el uso de su estacionamiento.

Escuela Enterprise Charter en Búfalo

Estudiantes y personal de la Enterprise Charter School[1] en Búfalo, NY, USA, utilizan RFID como medio para identificar y tener control de acceso a edificaciones. Esta escuela pública utiliza también esta tecnología para identificar y proteger los activos de esta como libros de biblioteca, computadoras portátiles, proyectores digitales, entre otros. Además de esto, los estudiantes pueden realizar compras en la cafetería con sus tarjetas de identificación.

Intuitek, empresa establecida en Búfalo, implementó las Tarjetas y Lectores RFID, y luego integró toda esta tecnología con el sistema de seguridad existente en la escuela. Los estudiantes presentan su tarjeta de ID en los kioscos asignados en la entrada de la escuela para informar de su llegada al plantel, esta información se guarda en la BD de la escuela y se reparte en tiempo real a los salones de clase.

Hotel Hilton London Kensington

Las instalaciones del Hotel Milton London Kensington[2] hacen uso de la tecnología RFID para la gestión de huéspedes. Se trata de un Sistema RFID, el cual consiste en entregar una tarjeta de Identificación con un chip integrado a los huéspedes del hotel a la hora de su arribo al mismo. Con esta tarjeta se van a abrir las puertas de las habitaciones a las que el huésped desee entrar, siempre y cuando se encuentren dentro del paquete o promoción que el huésped solicito, así mismo dará entrada a las piscinas, canchas de tenis, bares, restaurantes y galerías con las que cuenta el hotel.

Cada puerta del hotel cuenta con lectores que trabajan en la frecuencia de 125Khz para leer las tags de las tarjetas. Otra característica del sistema es que el personal del hotel puede rastrear en tiempo real la ubicación de los huéspedes.

Cadena de Tiendas Liverpool México

La cadena de tiendas departamentales Liverpool en México opto por instalar un sistema RFID en el año 2007 que va desde el centro de distribución hasta la tienda. Con este sistema el objetivo principal de la empresa es aumentar la satisfacción del cliente por medio de los siguientes beneficios:

[1] 275 Oak Street. Buffalo, New York 14203. (716) 855-2114
[2] London, GB,179-199 Holland Park Avenue, London GB W114UL

- Incrementar las ventas en tiendas acorde a reducción del OUT of STOCK
- Incrementar la eficiencia / productividad desde el centro de distribución hasta la tienda.
- Mejorar la experiencia de comprar. Mayor conocimiento del “Shopping” que los clientes experimentan

Las aéreas de mejora para encontrar los objetivos son:

- Mejorar la posibilidad del inventario físico
- Mejorar la conformidad del resurtido
- Reducir los errores en transacciones en el punto de venta
- Reducir los errores por devoluciones
- Cerrar errores de envíos a las tiendas
- Optimizar inventarios
- Reducir costos de operación
- Eliminar el manejo manual de los productos

El sistema se basa en la instalación de chips en todos los componentes que componen la cadena de distribución desde los camiones repartidores de los proveedores que deben ser identificados por los lectores instalados en las entradas de los almacenes de la cadena de tiendas departamentales, la validación del Pallet y sus cajas según el destino asignado mediante tags previamente instalados, el desempaquetado de los artículos y etiquetado con tags de acuerdo a pedidos previamente registrados en el Middleware que compone el sistema, en el cual interactúan todas las tiendas de la zona metropolitana de D.F, la recepción de en tienda previamente identificados los artículos y el control de inventarios mediante Hand Helds con RFID (Lectores RFID portátiles).

Cabe señalar que solo se aplica a la siguiente lista de artículos:

- Ropa
- Zapatos
- Farmacia/Perfumería
- DVD
- Electrónicos

Figura 2.14. Derecha Lectores RFID para lecturas de camiones repartidores de proveedores, Centro zona de etiquetado RFID para paquetes pedidos, Izquierda de etiquetas RFID en prendas ya colocadas en tienda

2.15 Prendas etiquetas con tags en estantes de tiendas Liverpool en la Ciudad de México

Figura 2.16. Discos de videojuegos y prendas etiquetas en estantes en tienda Liverpool en la Ciudad de México

3. Frecuencias

La frecuencia de utilización es el elemento más determinante en el momento de desplegar un sistema RFID, ya que depende de la frecuencia la adquisición del hardware necesario y el desarrollo del software de la aplicación.

Por ello en este apartado se realiza un análisis de las implicaciones que supone trabajar en las distintas frecuencias disponibles destinadas a esta tecnología.

3.1 Características a Considerar

Ya hemos visto que existen cuatro posibles frecuencias de funcionamiento: baja frecuencia, alta frecuencia, ultra alta frecuencia y frecuencia de microondas. En apartados sucesivos se va a proceder a realizar un análisis sobre las características de los sistemas RFID propias para cada rango. Previamente, se exponen las características que se van a considerar.

- *Capacidad de almacenamiento de datos*. Corresponde a la memoria de la etiqueta, para almacenar códigos o directamente datos.

- *Velocidad y tiempo de lectura de datos*. Es el parámetro que más se ve afectado por la frecuencia. En términos generales, cuanta más alta sea la frecuencia de funcionamiento mayor será la velocidad de transferencia de los datos. Esta circunstancia está estrechamente relacionada con la disponibilidad de ancho de banda en los rangos de frecuencia utilizados para realizar la comunicación. El ancho de banda del canal debe ser al menos dos veces la tasa de bit requerida para la aplicación deseada. Sin embargo, no es aconsejable seleccionar anchos de banda elevados, ya que según aumenta el ancho de banda aumentará también el nivel de ruido recibido, lo que redundará en una reducción de la relación señal a ruido. El tiempo de lectura dependerá lógicamente de la velocidad de lectura y de la cantidad de datos que hay que transmitir.

- *Cobertura*. Además de la frecuencia, la cobertura depende también de la potencia disponible en la etiqueta, de la aportada por la antena del lector y de las condiciones del entorno de la aplicación. El valor real será siempre función de estos parámetros y de la configuración final del sistema. Por este motivo, los valores que se presentan para cada banda, son meramente orientativos.

Se considera una cobertura pequeña los valores inferiores a 1 metro, mientras que las coberturas superiores a 1 metro se consideran altas.

- *Características de la zona de lectura*: orientación de la etiqueta, influencia de los obstáculos, influencia de las interferencias.
- *Costos*.
- *Áreas de aplicación más adecuadas*.

Rangos de frecuencias para Sistemas RFID		
Rango de Frecuencia	**Observaciones**	**Intensidad de Campo / Potencia**
135 KHz	Baja potencia. Acoplamiento inductivo.	72 dBµA/m
6.765 ... 6.795 MHz	Media frecuencia (ISM), acoplamiento inductivo.	42 dBµA/m
7.400 ... 8.800 MHz	Media frecuencia, usado sólo para EAS (Electronic Article Surveillance).	9 dBµA/m
13.553 ... 13.567 MHz	Media frecuencia (13.56 MHz, ISM), acoplamiento inductivo, ISO 14443, MIFARE, LEGIC..., smart labels (ISO 15693, Tag-It, ICode,...) y control de artículos (ISO 18000-3).	42 dBµA/m
26.957 ... 27.283 MHz	Media frecuencia (ISM), acoplamiento inductivo, sólo aplicaciones especiales.	42 dBµA/m
433 MHz	UHF (ISM), acoplamiento por backscatter, raramente usado para RFID.	10 ... 100 mW
868 ... 870 MHz	UHF (SRD), acoplamiento por backscatter, nueva frecuencia, sistemas bajo desarrollo.	500 mW, sólo Europa
902 ... 928 MHz	UHF (SRD), acoplamiento por backscatter, varios sistemas.	4 W – espectro ensanchado, sólo USA/Canadá.
2.400 … 2.483 GHz	SHF (ISM), acoplamiento por backscatter, varios sistemas, (identificación de vehículos: 2.446 .. 2.454 GHz)	4 W – espectro ensanchado, sólo USA/Canadá, 500 mW. Europa
5.725 ... 5.875 GHz	SHF (ISM), acoplamiento por backscatter, raramente usado para RFID.	4 W USA/Canadá, 500 mW Europa

Tabla 3.4 Rangos de frecuencia para RFID.

3.2 Sistemas de Baja Frecuencia 125 KHz

Los sistemas RFID de baja frecuencia suelen emplear etiquetas pasivas y utilizan para su funcionamiento el acoplamiento inductivo. Poseen pocos requisitos regulatorios.

Capacidad de datos

En el caso usual de etiquetas pasivas, la capacidad de datos es baja, de alrededor de 64 bits. Si se trata de etiquetas activas, éstas permiten una capacidad de almacenamiento de hasta 2 kbits.

Velocidad y tiempo de lectura de datos

Las tasas de transferencia de datos son bajas, típicamente entre 200 bps y 1 kbps. Por ejemplo, una etiqueta de 96 bits transmitiéndose a una velocidad de 200 bps, necesitará 0.5 segundos para ser leída, lo que implica un tiempo de lectura muy lento [17].

Cobertura

Al tratarse de un sistema inductivo, el campo magnético decrece muy rápidamente con la distancia (con el inverso del cubo de la distancia) y con las dimensiones de la antena. Este hecho puede verse como una ventaja en aplicaciones donde se requiera que la zona de cobertura esté estrictamente limitada a un área pequeña (en controles de producción).
Las antenas que utilizan son pequeñas y complejas, pero la tecnología está muy desarrollada.

Las etiquetas pasivas suelen poseer una cobertura pequeña, que alcanza como mucho los 0.5 metros, aunque depende también de la potencia disponible en la etiqueta.
Las etiquetas activas pueden superar los 2 metros, aunque este rango también depende de la potencia, construcción, configuración de la antena y tamaño.

Zona de lectura

La penetración en materiales no conductores es buena, pero no funcionan bien con materiales conductores. Este problema se incrementa con la frecuencia. Además son muy susceptibles a interferencias electromagnéticas industriales de baja frecuencia.

Costos

Dependen en gran medida de la forma y de las necesidades del sistema. En general, se puede decir que las etiquetas tanto activas como pasivas que se utilizan en los sistemas RFID de baja frecuencia son caras, en relación a aquellas que se utilizan en frecuencias superiores. Esto se debe a la naturaleza de los componentes utilizados, incluyendo la antena en espiral necesaria, y a

que los costos de fabricación son elevados en comparación con las etiquetas que trabajan a frecuencias superiores. Sin embargo, la construcción del chip y el encapsulado resulta más barato. Además, los lectores y programadores son simples y su costo de fabricación es menor que los de frecuencias más altas.

Áreas de aplicación

Aptas para aplicaciones que requieran leer poca cantidad de datos y para pequeñas distancias. Por ejemplo: control de accesos, identificación de animales, gestión de bienes, identificación de vehículos y contenedores, y como soporte a la producción.

El control de accesos es sin duda la aplicación más extendida para este intervalo de frecuencias. Sin embargo, hay que considerar la baja cobertura y pequeña capacidad de memoria de las etiquetas pasivas, por lo que para este tipo de aplicaciones en ocasiones puede ser necesario el empleo de etiquetas activas para ampliar la zona de lectura y poder mejorar la seguridad encriptado la información.

Las etiquetas de baja frecuencia también aparecen en la identificación animal con el fin de: gestionar el ganado, identificar y controlar las especies protegidas o identificar animales domésticos.

3.3 Sistemas de Alta Frecuencia 13,56 MHz

Hoy en día, la mayoría de los sistemas RFID que funcionan a 13.56MHz son pasivos, lo cual implica la no necesidad del uso de baterías. Esto tiene ventajas en cuanto al costo, tiempo de vida de las etiquetas y entorno en que se pueden emplear estos sistemas. El principio básico de operación es la transmisión de energía y datos usando acoplamiento inductivo. Este es el mismo principio que usan los transformadores.

A diferencia de otros sistemas de RFID que trabajan a frecuencias más altas (por ejemplo dentro de la banda UHF o microondas), los sistemas a 13.56MHz (e incluso los que trabajan a <135KHz) tienen la zona de operación en el campo creado junto a la antena del lector, lo que permite alcanzar unas distancias del orden del diámetro de la antena. Hay que tener en cuenta que esto es así siempre que estemos trabajando con sistemas con una sola antena.

Para distancias mayores al equivalente al diámetro de la antena, la intensidad del campo decrece con la tercera potencia de la distancia, lo cual significa que la potencia de transmisión requerida se incrementa con la sexta potencia de la distancia.

La Figura 3.1 muestra la dependencia de la intensidad del campo, normalizada, en función de la distancia para antena con un diámetro de 0.8m.

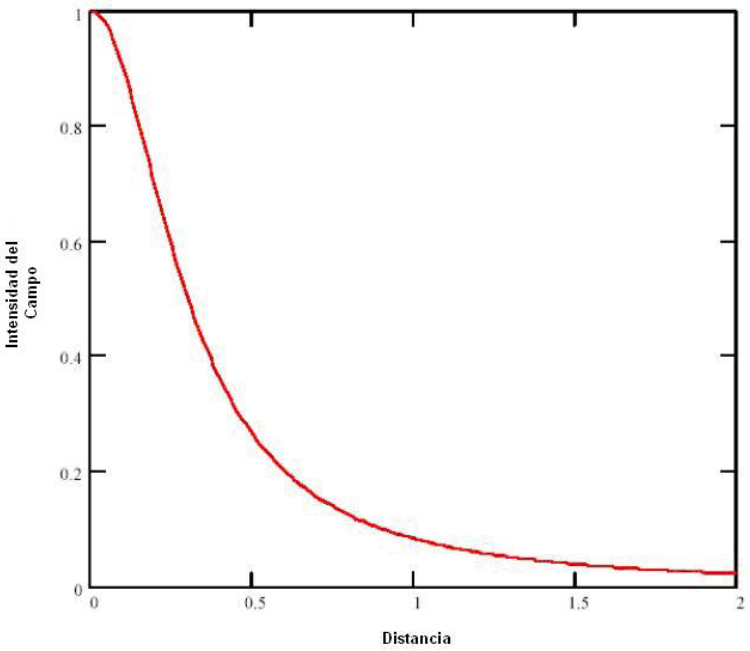


Figura 3.1 Comportamiento de la intensidad de campo en función de la distancia

A diferencia que en los sistemas de RFID que usan frecuencias dentro del rango de UHF o microondas, la radiación emitida a 13.56MHz no es absorbida por el agua ni la piel humana, lo que permite que las ondas se propaguen con mayor facilidad puesto que la influencia del agua o las personas en su comportamiento es insignificante.

Debido a los efectos de blindaje o reflexión, los sistemas de RFID son sensibles a los metales dentro del campo de operación. Esto afecta a todos los sistemas de identificación por radiofrecuencia, aunque los motivos físicos son diferentes para cada caso concreto.

El hecho del que el campo magnético sea un campo vectorial implica que la orientación del tag tiene influencia dentro del mismo. Esta influencia de la orientación puede resolverse mediante el uso de antenas de transmisión más complejas (por ejemplo, mediante el uso de campos rotantes). Así es posible trabajar con las etiquetas independientemente de su orientación dentro de la zona de operación.

Debido también a que los sistemas RFID inductivos operan a distancias cortas, la influencia de sistemas adyacentes o ruidos externos es mucho menos que en sistemas que trabajan en la zona UHF o microondas (debido a que la potencia decrece con el cuadrado de la distancia, cuando a 13.56MHz decrece con la sexta potencia de la distancia).

Etiquetas típicas

Hoy en día las etiquetas a 13.56MHz están disponibles en muchas formas y con diferentes funcionalidades. Por supuesto esto ha sido muy influenciado por las aplicaciones y sus requerimientos. El hecho de que unas pocas vueltas de la antena de la etiqueta (habitualmente menos de 10) sean suficientes para lograr una etiqueta con un buen funcionamiento es uno de los beneficios reconocidos para permitir la producción de tags a bajo costo basados en diferentes tecnologías de antena.
Hay tres tipos principales de tags a 13.56MHz:

- Tarjetas ISO:

- ISO 14443: son “Tarjetas de identificación- Proximity integrated circuit cards”. Con un rango entre 7-15 cm, usadas principalmente en el campo de la expedición de tickets.
- ISO15693: son “Tarjetas de identificación- Contactless integrated circuit cards”. Con un rango superior a 1 m, usadas principalmente en los sistemas de control de acceso.
- Tags rígidos industriales para logística
- Etiquetas inteligentes, delgadas y flexibles.

Funcionalidad

- Tamaño de la memoria: típicamente desde 64 bits (en dispositivos simples de identificación) hasta varios kilobytes (empleados en tarjetas inteligentes).
- Tipo de memoria: programadas de fábrica, de sólo lectura (típicamente en identificación y pequeña memoria), sólo programables una vez (OTP) y de lectura/escritura (permitiendo la modificación de datos).
- Seguridad: básicamente todos los niveles de seguridad se pueden alcanzar. En el caso, por ejemplo, de aplicaciones en las que haya una transferencia de dinero se requieren los niveles más altos de seguridad.
- Capacidades multitag: resueltas y soportadas por la mayoría de los nuevos productos.

Tipos de lector

Sin lugar a dudas la etiqueta tiene una gran importancia dentro de un sistema RFID, sin embargo el lector tiene la misma importancia dentro de un sistema RFID de índole profesional. La parte principal del interrogador es un módulo de radiofrecuencia encargado de la comunicación entre él y el tag. Hay diferentes dispositivos, los principales son:

- Módulo RF para aplicaciones de “proximidad” (hasta 100mm). Se emplean en dispositivos portátiles, impresoras y terminales. Esta funcionalidad se puede integrar en un circuito impreso, permitiendo módulos de reducido tamaño y reducción de costos.

- Módulo de RF para aplicaciones de “vecindad” (amplio rango, en el caso de 13.56MHz hasta 1.5m). Son más complejos que los módulos de “proximidad”, tienen un mayor consumo de potencia y una circuitería más compleja.

- También se puede encontrar en ocasiones una tercera clase, de “medio rango” para distancias de hasta 400mm.

Los interrogadores fijos suelen colocarse a lo largo de las líneas de producción para identificar y hacer el seguimiento de los objetos. En algunas aplicaciones es necesario blindar los interrogadores para protegerlos de perturbaciones externas. Los lectores con forma de puerta se emplean en almacenes, establecimientos y bibliotecas para EAS (Electronic Article Surveillance).

También existen interrogadores que emplean múltiples antenas que permiten extender el rango de cobertura y leer los tags en cualquier orientación. Existe la posibilidad de emplear protocolos anticolisión que permiten la lectura de múltiples tags simultáneamente dentro del campo de la antena. Dependiendo del protocolo y la configuración empleada pueden leerse hasta 30 tags por segundo, lo que equivale a leer los tags colocados uno detrás de otro separados una distancia de 0.1m y desplazándose a 3m/s [18].

Capacidad de datos

Las etiquetas (pasivas) suelen poseer capacidades típicas que van desde 512 bits (frecuentemente portan un número unívoco de identificación industrial de 64 bits) hasta 8
kbits, divididos en sectores o bloques que permiten direccionar los datos.

Velocidad y tiempo de lectura de datos

Típicamente la velocidad de datos suele ser de unos 25 Kbps (menor si se incluyen algoritmos de comprobación de errores de bit). También están disponibles dispositivos con tasas mayores de 100 Kbps
Los sistemas RFID a esta frecuencia son capaces de leer aproximadamente 40 etiquetas por segundo. Por ejemplo 512 bits transmitiéndose a 25 Kbps tardan aproximadamente 0.02 segundos. Por tanto en leer 40 etiquetas, se empleará 1 segundo.

Cobertura

Típicamente las etiquetas pasivas poseen un radio de cobertura de alrededor de 1 metro.

Zona de lectura

Posee una buena penetración en materiales y líquidos no conductores. Sin embargo, no funciona bien cuando existen materiales metálicos en la zona de lectura, ya que éstos producen reflexiones

en la señal. Su inmunidad al ruido por interferencias electromagnéticas industriales de baja frecuencia es mejor que para los sistemas de Baja Frecuencia.
La orientación de la etiqueta puede resultar otro problema según aumenta la distancia, debido a las características vectoriales de los campos electromagnéticos. Este efecto puede contrarrestarse mediante la utilización de antenas de transmisión más complejas.

Costos

Depende principalmente de la forma de la etiqueta y de su aplicación. El diseño de la antena del tag es sencillo, por lo que su costo es menor que a BF.

Los sistemas RFID que utilizan tarjetas inteligentes son los más baratos dentro de la categoría de alta frecuencia.

Áreas de aplicación

Al igual que en BF, los sistemas de AF son aptos para aplicaciones que requieran leer poca cantidad de datos y a pequeñas distancias. Es el caso de la gestión de maletas en aeropuertos, bibliotecas y servicios de alquiler, seguimiento de paquetes y aplicaciones logísticas en la cadena de suministros.

Funcionamiento

Que el sistema funcione es una de las principales cuestiones dentro de los requerimientos de las aplicaciones. Así la meta es cumplir con el propósito de tener un sistema con un funcionamiento bueno dentro de una probabilidad elevada. Mientras que las cuestiones funcionales como el tamaño de la memoria o nivel de seguridad pueden ser seleccionadas teniendo en cuenta los requerimientos de las aplicaciones, algunos otros parámetros clave (rango, fiabilidad y velocidad de la comunicación) están sujetos a leyes físicas y, por lo tanto, muestran cierta independencia. Típicamente las distancias más pequeñas permiten velocidades mayores (los sistemas de “proximidad” operan aproximadamente a 100kBaud o más), mientras que distancias mayores sólo se pueden lograr con velocidades más lentas (entre 25 y 70kBaud).

Esto tiene un impacto en la integración y la optimización del sistema. Sin embargo, existe la evidencia de que los sistemas RFID a 13.56MHz pueden alcanzar aproximadamente 1.5m sin problemas en aplicaciones “puerta” o cubrir una “ventana” de 1x1m en un “lector túnel” y solucionan los requisitos clave de las aplicaciones en términos de tamaño de datos y movilidad de objetos. Estas ideas están basadas en tags del tamaño de una tarjeta de crédito.

El funcionamiento no está tan sólo fijado por las regulaciones y por la velocidad de transmisión sino que también depende de la sensibilidad o robustez que tiene al ruido.

Debido a que la señal del transponder puede ser transmitida por una subportadora que opera fuera de la (ruidosa) banda ISM, el funcionamiento del sistema puede ser muy estable comparado, por ejemplo, con los sistemas a <135kHz. La robusteza al ruido puede ser realzada por receptores selectivos y por el hecho de que ambas subportadoras pueden ser procesadas independientemente en sistemas de alto rendimiento.

Esto da una idea de la “ventana de funcionamiento” de los sistemas que trabajan a 13.56MHz. Evidentemente, el funcionamiento final depende de muchos factores que deben ser optimizados para cada aplicación concreta.

3.4 Sistemas de Ultra Alta Frecuencia (UHF) 433MHz, 860MHz, 928MHZ

Los sistemas RFID que trabajan a Ultra Alta Frecuencia basan su funcionamiento en la propagación por ondas electromagnéticas para comunicar los datos y para alimentar la etiqueta en caso de que ésta sea pasiva.

Principios de Operación

Los sistemas de RFID que operan en el rango de frecuencias de UHF emplean la propagación convencional de una onda electromagnética para la comunicación y alimentación de tags no alimentados por batería. Este funcionamiento difiere del de los sistemas a bajas frecuencias que usan la inducción electromagnética, más similar a los transformadores.

El lector emite una onda electromagnética que se propaga con un frente de onda esférico. Las etiquetas colocadas dentro del campo recogen parte de la energía de la onda emitida. La cantidad de energía disponible en un punto está relacionada con la distancia que hay desde el punto emisor y decrece con la segunda potencia de la misma (es decir, que E es proporcional a
1/d2). En la figura 3.2 se representa la anterior explicación

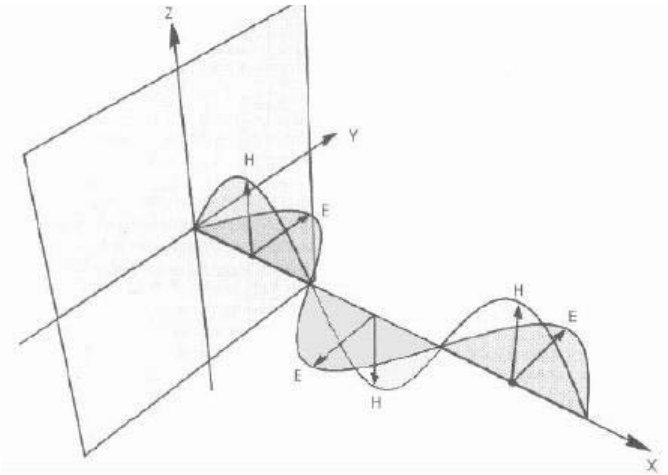


Figura 3.2 Propagación de una onda electromagnética. E y H son perpendiculares y están en fase la una con la otra.

La cantidad de energía recibida es función de la apertura de la antena receptora, lo que en términos simples es lo mismo que decir que depende de la longitud de onda de la señal recibida. Consideremos, por ejemplo, una antena de media de longitud de onda para 300MHz (0.5 m) y de 0.25m a 600MHz. El área activa alrededor de la antena tiene la forma de una elipse.

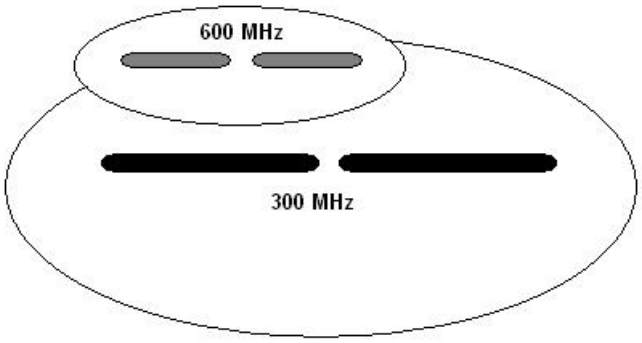


Figura 3.4 Área activa para antenas de 300 y 600MHz.

Como se observa en la Figura 3.4, el área de la elipse de la antena a 300MHz es cuatro veces la de la antena a 600MHz. De esta forma el área de captación de energía a 300MHz es cuatro veces la de 600MHz.

La antena receptora puede ser físicamente más pequeña y, aún así, tener la misma apertura ya que existen compensaciones para reducir el tamaño de la antena como reducir el ancho de banda o un ajuste más fino. En la práctica, el rango de trabajo depende de la energía que radia el lector, de la frecuencia de trabajo y del tamaño de la antena de la etiqueta.

Para que la tecnología RFID pasiva sea correctamente explotada el lector debe producir un adecuando campo magnético para alimentar las etiquetas a una distancia que sea útil. Atendiendo

a las regulaciones actuales, que son más restrictivas en Europa, la potencia radiada está limitada a 500mW, lo que se traduce en un rango de lectura de unos 0.7m a 870MHz. En EEUU y Canadá se permite una potencia radiada de 4W, lo que se traduce en un rango del orden de 2m. Existen licencias especiales en Estados Unidos que permiten una potencia que supera los 5m.

Funcionamiento

Cuando se realiza una transmisión en RF, hay diversos factores que pueden influir en el correcto funcionamiento de la comunicación entre emisor y receptor.

Absorción, Reflexión, refracción y difracción

Una onda electromagnética puede verse afectada por alguno de estos cuatro factores, esto puede provocar que la comunicación no se realiza correctamente. Por tanto el estudio de estos factores y de cómo afectan cada uno a las características de las ondas electromagnéticas es estudiado en cada caso.

Por ejemplo, la absorción depende de las características del material a través del cual la onda se propaga. La absorción de energía se produce debido a que parte de esta energía se disipa en el material que opone una resistencia al paso de la onda.

Las ondas electromagnéticas son afectadas también por el fenómeno de refracción y difracción, cuando estas ondas pasan por diferentes medios o cuando inciden en el borde de un objeto. Las transmisiones a frecuencias más elevadas son más propensas a este tipo de fenómenos.

Las ondas electromagnéticas se pueden reflejar en una superficie conductora como un metal, agua, hormigón, etc. La reflexión puede provocar que la transmisión se anule completamente, pero también puede beneficiarla. Todo dependerá de cómo se encuentran la onda reflejada y la onda directa, en fase o contratase. Podemos apreciarlo en la Figura 3.5

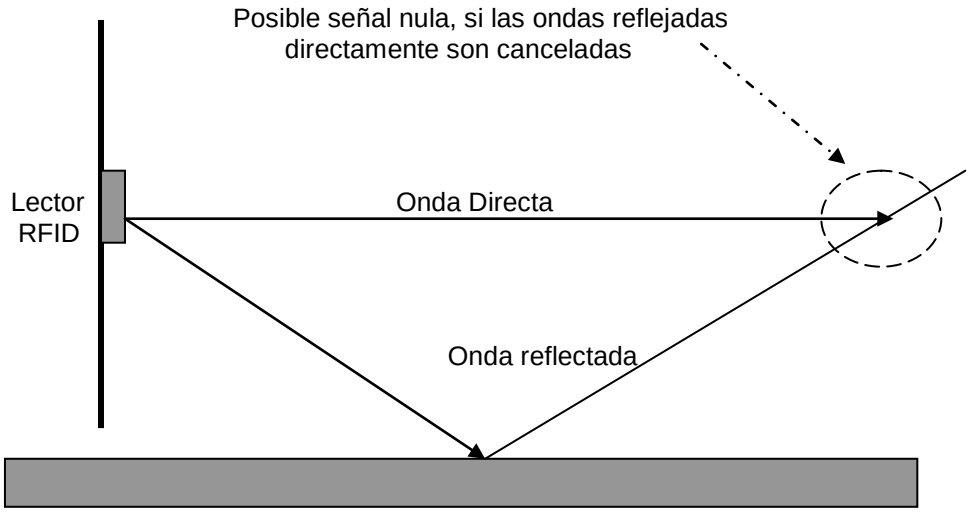


Figura 3.5 Esquema de la propagación de una onda electromagnética y su onda reflejada

Penetración en líquidos

Las ondas de radio penetran en diferentes líquidos dependiendo de la conductividad eléctrica del líquido en el cual penetran. Por ejemplo, el agua tiene una alta conductividad eléctrica y, por tanto, tiende a reflejar y absorber energía electromagnética mientras que el aceite o el petróleo tienen una baja conductividad permitiendo el paso a través de ellos con unos niveles relativamente bajos de atenuación.

Rango de lectura

El rango de lectura depende de la potencia de transmisión y, en el caso de los tags pasivos, también los requerimientos de energía de los mismos. El rango efectivo de lectura depende también del factor de absorción del material al cual va unido el tag.
El tamaño del tag también juega un papel importante en el rango de lectura. Cuanto menor es el tag, menor es el área de captura de energía, por lo que menor es el rango de lectura. Un diseño adecuado del sistema, la optimización de la potencia del lector, la orientación de la antena y una colocación óptima del tag ayudan a superar estas limitaciones.

Interferencias

El ruido eléctrico procedente de motores, luces fluorescentes, etc., es mínimo en UHF. De mayor consideración es el efecto de otros sistemas RFID, teléfonos móviles, aparatos que trabajen en la banda ISM, etc. Aunque la mayoría de estas fuentes de señal emiten en una banda muy estrecha.
FHSS (Frequency hopping spread spectrum) es una de las formas más efectivas de reducir los efectos de las interferencias y de reducir las interferencias sobre otros dispositivos que comparten el espectro. De este modo la energía transmitida se distribuye a lo largo de la banda de frecuencias, reduciendo las posibles interferencias creadas a otros sistemas y, así, como la frecuencia del receptor está continuamente cambiando, evita los efectos de otros usuarios bloqueando el receptor.

Capacidad de lectura direccional

La naturaleza de las ondas de UHF permite el uso de pequeñas antenas direccionales. Esto permite dirigir el rayo del interrogador hacia un área en particular y poder leer selectivamente un grupo de tags y evitar la lectura de otros. Esta capacidad de direccionabilidad tiene otra ventaja, que es la de permitir que el interrogador evite zonas con posibilidad de interferencias.

Orientación de la etiqueta

La orientación de la antena de la etiqueta con respecto a la antena del interrogador influye en el rango de lectura. Cuando la onda electromagnética está polarizada linealmente, la antena del tag debe estar orientada en la misma dirección que la del interrogador para permitir la máxima

reopción de energía. La situación de peor caso se da cuando la orientación entre ambas antenas forma un ángulo recto. Si la onda electromagnética no está polarizada linealmente no importa la orientación que tenga la antena de la etiqueta. Por ejemplo, si empleamos una onda electromagnética polarizada circularmente podemos emplear cualquier orientación para el tag.

Capacidad de datos

Están disponibles etiquetas activas y pasivas con capacidades típicas desde los 32 bits (frecuentemente portan un número unívoco de identificación) hasta los 4 Kbits, típicamente divididos en páginas de 128 bits para permitir direccionar los datos.

Velocidad y tiempo de lectura de datos

La velocidad de transferencia de datos está típicamente alrededor de 28 kbps (menor si se incluyen algoritmos de comprobación de errores de bit) pero también están disponibles velocidades mayores.
Permite la lectura de aproximadamente 100 etiquetas por segundo. Por ejemplo 32 bits transmitidos a 28 Kbps tardan 0.001 segundos. Por tanto en leer 100 etiquetas se emplearán 0.1 segundos.

Cobertura

Las etiquetas de UHF pasivas pueden alcanzar una cobertura de 3 ó 4 metros. Trabajando con etiquetas activas y a la frecuencia más baja, 433 MHz, la cobertura puede alcanzar los
10 metros.

Sin embargo, la cobertura está significativamente influenciada por las regulaciones de los distintos países correspondientes a la cantidad de potencia permitida, que es menor en Europa que en Estados Unidos. La estandarización es insuficiente y la tecnología poco madura.

Sin ir más lejos, en Europa, donde la potencia máxima emitida por el lector es de 0.5 Watios, el alcance del sistema puede reducirse hasta los 33 centímetros. Se espera que este valor se incremente hasta los 2 metros, cuando la potencia máxima permitida aumente hasta 2 Watios.

Zona de lectura

Posee una buena penetración en materiales conductores y no conductores, pero presenta dificultades ante la presencia de líquidos (agua). Su inmunidad al ruido por interferencias electromagnéticas industriales de baja frecuencia es mejor que para los sistemas de baja frecuencia, pero debe considerarse la influencia de otros sistemas de UHF operando en las proximidades.

La orientación de la etiqueta también puede resultar un problema a esta frecuencia, debido a las características vectoriales de los campos electromagnéticos. Este efecto puede contrarrestarse mediante la utilización de antenas de transmisión más complejas.

Costos

Los costos dependen principalmente de la forma. Las tarjetas inteligentes presentan un costo razonable, representando la opción más barata dentro de la categoría de sistemas RFID UHF. En grandes cantidades, estos tags a UHF pueden ser más baratos que los de frecuencias más bajas.

Áreas de aplicación

Apta para aplicaciones que requieran distancias de transmisión superiores a las bandas anteriores, como en la trazabilidad y seguimiento de bienes y artículos, y logística de la cadena de suministros.

3.5 Sistemas en Frecuencia de Microondas 2.45 y 5.8 GHz

Principios de operación

Los sistemas RFID en el rango de las microondas se vienen usando desde hace más de 10 años en aplicaciones de transporte (seguimiento de vehículos por vías o raíles, peajes y otro tipo de control de acceso a vehículos). Los sistemas que operan en la banda UHF y en la región de microondas se dividen en “activamente alimentados” y “pasivamente alimentados”. El rango de operación y la funcionalidad son superiores en los tags activos (con una batería en el tag) mientras que un bajo costo y un mayor tiempo de uso son las ventajas de los tags pasivos.

En el pasado las etiquetas para microondas eran bastante complejas y caras debido al desafío de procesar señales de microondas con circuitos integrados CMOS.
Actualmente, la mayoría de estos dispositivos para seguimiento de artículos usan un único circuito integrado y alimentación pasiva. Esto conlleva ventajas en cuando a costo y tiempo de vida.
El principio básico de operación a 2450MHz consiste en la transmisión de datos y energía usando la propagación de señales de radio Una antena en el interrogador genera una onda electromagnética que es recibida en la antena el tag. En un tag pasivo se convierte esta señal recibida en un voltaje DC para alimentarse. La transmisión de datos desde el lector hacia un tag se lleva a cabo cambiando algún parámetro de la onda transmitida (amplitud, fase o frecuencia).
La transmisión de retorno desde el tag hacia el interrogador se lleva a cabo cambiando la carga de la antena del tag (amplitud y/o fase). En este contexto, los sistemas que trabajan por debajo de 135KHz, a 13.56MHz y en microondas usan el mismo principio. Para los sistemas RFID de microondas este método se llama “modulated backscatter”. De forma alternativa, se puede generar

otra señal de diferente frecuencia y modularla para transmitirla al interrogador. Los sistemas que usan este último método emplean tags transmisores RF activos [19].

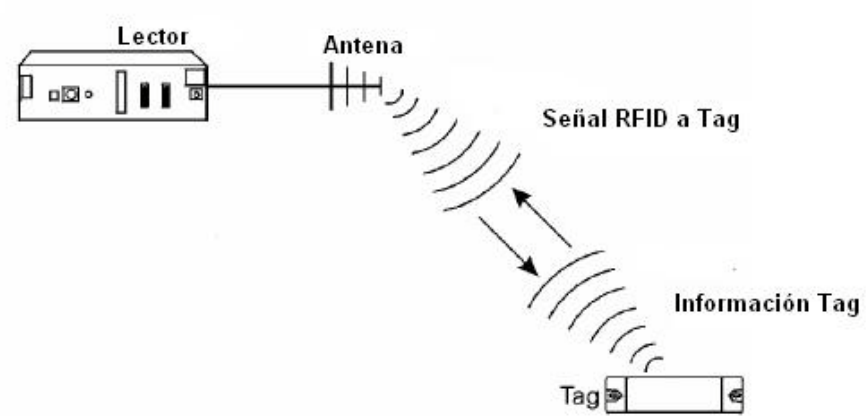


Figura 3.6 Principio básico de los sistemas RFID que trabajan con microondas

A diferencia de los sistemas RFID inductivos (13.56MHz y <135KHz), los sistemas de UHF y microondas operan en el "campo lejano" de la antena de transmisión del interrogador. Las distancias alcanzables para tags pasivos están entre los 0.5 y los 12m y más allá de los 30m para los tags activos, dependiendo de la frecuencia de microondas, las regulaciones del país o región donde trabaja y las características de la antena. Como los tags operan en el "campo lejano" de la antena del interrogador, la intensidad de este campo decrece con la primera potencia de la distancia (es decir, E es proporcional a 1/d).

Las ondas en UHF y microondas se atenúan y reflejan en materiales que contienen agua o tejidos humanos y se reflejan en objetos metálicos. Al contrario que en los sistemas RFID inductivos, es posible diseñar tags que trabajen unidos a objetos metálicos. También atraviesan fácilmente madera, papel, ropa, pintura, suciedad, etc.

Adicionalmente, debido a la corta longitud de onda de las señales de radio empleadas y a las propiedades de reflexión de los objetos metálicos, los sistemas lectores se pueden diseñar para tener una alta capacidad de lectura en zonas con gran contenido en objetos metálicos.

Como el campo eléctrico es un campo vectorial, existe una relación entre la orientación del tag y la distancia de lectura. El impacto de esta dependencia de la orientación se puede solucionar mediante el empleo de antenas más complejas sin que influya así la orientación de la etiqueta.

Etiquetas típicas

En la actualidad los tags de 2450MHz están disponibles en muy diferentes formatos en cuanto a forma y funcionalidad. A diferencia de los sistemas RFID inductivos, los cuales requieren bastante área o bastantes vueltas de cable o incluso un núcleo magnético para recoger el campo magnético, los tags de UHF y los de microondas pueden ser muy pequeños requiriendo sólo una determinada longitud en una sola dimensión. Por eso los tags son más fáciles de encapsular. Tamaños típicos son de 2 a 10 cm.

Forma

Hay dos clases de tags para los 2450 y 5800MHz:

- Tags industriales rígidos para usos logísticos.
- Etiquetas finas y flexibles.

Las expectativas son que en el futuro se empleen muchos más tipos diferentes de etiquetas. Esta es una ventaja de los tags de 2450MHz, que se pueden conseguir una gran variedad de formas y tamaños.

Funcionalidad

El tamaño de la memoria (como en todas las frecuencias) está limitado sólo por el costo. Es posible conseguir una gran oblea con una capacidad del orden de Kb, pero el costo se incrementa de acuerdo con ello. Las memorias típicas suelen estar entre los 64 bits (aplicaciones simples para identificación) y algunos Kb (empleadas en aplicaciones logísticas con gran cantidad de datos).
En cuanto a la seguridad, se pueden conseguir todos los niveles de seguridad deseados (desde niveles bajos para una simple tarea de control hasta los más elevados para tareas de transferencias económicas, por ejemplo).

Funcionamiento

Hay que tener en cuenta que si hablamos de sistemas activos, las velocidades de transmisión no dependen en gran medida de si empleamos UHF o microondas, mientras que para tags pasivos, los bajos requisitos de consumo para el mismo exigen unas velocidades de transmisión bajas. Los sistemas de amplio rango de lectura (distancias mayores a 15m) operan a velocidades de hasta 1Mbit/s. Los tags pasivos de UHF y microondas operan típicamente a velocidades entre 10 y 50Kbits/s.

Capacidad de datos

Están disponibles sistemas de etiquetas activas y pasivas, con capacidades que van típicamente desde 128 bits hasta dispositivos de 512 Kbits, que pueden dividirse en sectores o bloques para permitir direccionar los datos.

Velocidad y tiempo de lectura de datos

Depende del diseño de la etiqueta, pero suele ser elevada. La velocidad típica está por debajo de los 100 kbps, aunque algunos dispositivos pueden alcanzar 1 Mbps Por ejemplo 32 kbits transmitidos a 100 kbps tardan 0.3 segundos. Si lo que mide son bloques de 128 bits, de 40 etiquetas, se emplearán 0.05 segundos.

Cobertura

Abarcan regiones de entre 1 y 2 metros para dispositivos pasivos y hasta 15 metros o más, para dispositivos activos.

Zona de lectura

Posee una buena penetración en materiales no conductores, pero no así en líquidos que contienen agua, donde el coeficiente de absorción es importante. Es reflejado por metales y otras superficies conductoras. Es susceptible al ruido. Se trata de una banda de trabajo compartida.

Costos

Los costos dependen principalmente de la forma y el modo de alimentación (activo/pasivo).

Áreas de aplicación

Apta para aplicaciones que requieran alta cobertura y velocidades de transmisión elevadas.
Por ejemplo: automatización en la fabricación, control de accesos, peaje de carreteras, logística de la cadena de suministros y aplicaciones logísticas militares.

A continuación se realiza una comparativa de las características de las etiquetas, dependiendo del intervalo de frecuencia de trabajo.

PARÁMETROS	BAJA FRECUENCIA (<135KHz)	ALTA FRECUENCIA (13.56KHz)	ULTRA ALTA FRECUENCIA (433MHz, 860MHz,928MHz)	FRECUENCIAS MICROONDAS (2.45 GHz, 5.8GHz)
Cobertura	**Menor**			**Mayor**
Tamaño de la Etiqueta	←	—	—	→
Velocidad de Lectura de Datos	←	—	—	→
Lectura en Presencia de Líquidos o Metales	←	—	—	→
Lectura en Presencia de Inferencias EM	←	—	—	→

Tabla 3.2. Comparativa de las características asociadas a cada rango de frecuencia

3.6 Comparativa con tecnologías competidoras

En el ámbito de las tecnologías de identificación automática existen otras alternativas a RFID. Por un lado están las tecnologías de identificación y captura de datos que se han venido utilizando hasta ahora, entre las que destaca claramente el código de barras, que ya ha alcanzado un alto grado de madurez y de penetración en el mercado. Por otro lado aparecen nuevas tecnologías aún bajo estudio o incluso en sus primeros estadios de fase de implantación, algunas de las cuales se basan en ondas de radio (como RFID) y otras en lectores láser (como el código de barras).

En primer lugar vamos a comparar RFID con dos de las tecnologías de identificación competidoras que ya existen y están disponibles en el mercado: los códigos de barras y los botones de contacto. Las características que utilizaremos para realizar la comparación son:

- Posibilidad de modificar los datos.
- Seguridad de los datos.
- Cantidad de datos almacenados.
- Costos.
- Estándares.
- Vida útil.
- Distancia de lectura.
- Número de elementos que se pueden leer simultáneamente.
- Posibilidad de interferencias.

3.6.1 Códigos de Barras

El código de barras se basa en la representación de la información mediante un conjunto de líneas paralelas verticales de distinto grosor y espaciado. De este modo, el código de barras permite, por ejemplo, reconocer rápidamente un artículo en un punto de la cadena logística y así poder realizar inventario o consultar sus características asociadas. Actualmente, el código de barras está implantado masivamente de forma global. Los códigos de barras presentan diversas ventajas, como son la facilidad de implementación, bajo costo y amplia madurez y disponibilidad de productos. Como contrapartida, los códigos de barras presentan diversos inconvenientes como su limitación de una única lectura cada vez, es decir, no se pueden leer varios códigos de barras de forma simultánea, o que únicamente se puede almacenar un código de información, sin poder añadir datos adicionales. Además, requieren línea de visión física para realizar la lectura así como que el código esté en la orientación adecuada.

Existen tres tipos principales de códigos:

- Códigos lineales.
- Códigos de barras 2-D.
- Códigos matriciales.

Seguidamente analizamos los tres tipos desde el punto de vista de las características mencionadas anteriormente.

Códigos lineales

Son los tradicionales códigos de barras. Ampliamente utilizados desde hace tiempo, se pueden encontrar hoy en día en cualquier tipo de producto. Están formados por una serie de bandas verticales alternando negras y blancas. En el patrón que forman se encuentra codificada la información. Su lectura se realiza mediante un escáner LED o Láser.

Figura 3.7 Código de barras.

- *Posibilidad de modificar los datos*. No existe. Una vez impreso el código de barras, no se puede modificar.
- *Seguridad de los datos*. No usan cifrado, y el estándar es bien conocido.
- *Cantidad de datos almacenados*. Pueden almacenar hasta 30 caracteres.
- *Costos*. muy bajos.
- *Estándares*. Aunque existen más de 200 esquemas diferentes de códigos de barras en uso, existen cuatro tipos dominantes: UPC/EAN, Interleaved 2-of-5, Código 39 y Código 128, y se encuentran cubiertos por la *International Organization for Standarization* (ISO).
- *Vida útil*. Baja, pues se trata de información impresa que tiende a borrarse con el tiempo, aunque se pueden proteger.
- *Distancia de lectura*. Necesitan línea de visión, por lo que la lectura debe ser cercana (del orden de un metro).
- *Número de elementos que se pueden leer simultáneamente*. Sólo se puede leer un código cada vez.
- *Posibilidad de interferencias*. Los códigos de barras no suelen tener corrección contra errores, y los daños físicos en la etiqueta del código pueden imposibilitar su lectura. Además son sensibles al polvo y a la suciedad, tanto en la etiqueta como en las lentes del lector.

Códigos de barras 2-D

Estos códigos consisten en una pila de códigos de barras muy cortos dispuestos ordenadamente para su descodificación. El estándar más utilizado es PDF 417.

Figura 3.8. Ejemplo de código de barras 2-D con el estándar PDF 417. Fuente: BarCode 1.

Sus características son muy semejantes a las del código lineal. Sus principales diferencias son:

- *Seguridad de los datos*. Emplean corrección de errores mediante códigos Reed- Solomon, con lo que se podría destruir parte de la etiqueta sin destruir la información.
- *Cantidad de datos almacenados*. Pueden almacenar hasta 1 Kbyte.
- *Costos*. Muy bajos.
- *Estándares*. PDF 417 es un estándar de ISO.
- *Posibilidad de interferencias*. Son más robustos a los errores de lectura que los códigos lineales, aunque cantidades importantes de polvo o suciedad los pueden inutilizar por completo.

Códigos matriciales

Están formados por elementos simples (puntos o cuadrados) dispuestos formando un modelo bidimensional. Éstas son las diferencias fundamentales con el código de barras lineal:

- *Seguridad de los datos*. Semejante a la de los códigos de barras 2-D.
- *Cantidad de datos almacenados*. Semejante a la de los códigos de barras 2-D.
- *Costos*. Más altos que los anteriores.
- *Estándares*. Existen diferentes estándares, pero los más importantes son: Data Matrix, códigos QR y MaxiCode.

Figura 3.9 Código QR.

3.6.2 Botones de Contacto

Aunque no se trata de una tecnología muy extendida, y cuenta con pocos suministradores, ha tenido cierta utilización y es potencialmente alternativa a la RFID, por lo que la comentaremos en este apartado. Requiere contacto físico entre el lector y la etiqueta en forma de botón para realizar la lectura.

Figura 3.10 Brazalete médico con memoria de botón.

Figura 3.11 Ejemplo de dispositivo lector.

Sus características más relevantes son:

- *Posibilidad de modificar los datos*. La información almacenada en un botón puede leerse y escribirse muchas veces.
- *Seguridad de los datos*. Los datos pueden estar cifrados.
- *Cantidad de datos almacenados*. Hasta 8 MB.
- *Estándares*. Se trata de tecnologías propietarias, y no existe un estándar aceptado universalmente.
- *Vida útil*. Al requerirse contacto físico, la vida útil queda limitada.
- *Distancia de lectura*. Se requiere contacto físico entre el lector y la etiqueta.
- *Número de elementos que se pueden leer simultáneamente*. Sólo se puede leer una etiqueta cada vez.
- *Posibilidad de interferencias*. Al requerirse contacto físico, el peligro de interferencias es menor.

3.7 Tecnologías Competidoras Emergentes

Como ya hemos comentado, existen otras tecnologías aún en fase emergente, que pueden considerarse competidoras de RFID por ofrecer funcionalidades parecidas. A continuación se describen brevemente.

3.7.1 Surface Acoustic Waves (SAW - Ondas Acústicas de Superficie).

La principal ventaja de la tecnología SAW es la posibilidad de disponer de etiquetas de lectura a muy bajo costo, principalmente gracias a que no requiere un chip de procesado. Su funcionamiento es el siguiente: una vez que el tag recibe la señal radio del lector, un simple transductor en el tag la

convierte en onda acústica, que incide sobre la superficie metálica construida sobre él a tal efecto (ver Figura 3.12).

Esta superficie reacciona según un patrón preestablecido, reflejando la señal acústica de vuelta hacia el transductor que la convierte de nuevo en señal de radio.
El efecto final es muy similar al de RFID pero, al no requerir chip de procesado, el costo es significativamente menor. Otra ventaja es que funciona muy bien en presencia de líquidos y metales, al contrario que RFID en HF y UHF. Como inconvenientes aparece que las etiquetas no son modificables (se codifican en fabricación) y que aún existen problemas para evitar colisiones entre lecturas.

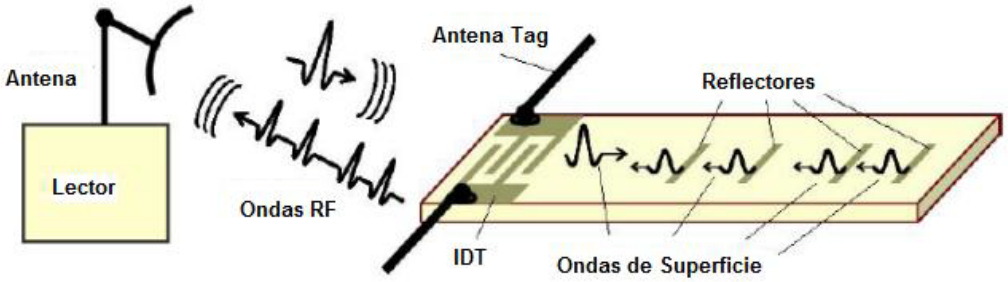


Figura 3.12 Funcionamiento de SAW.

- *Tags celulares.* El etiquetado celular tiene el inconveniente de que las células mueren y por ello es preciso reemplazar el tag frecuentemente. Sin embargo, este tipo de etiquetado es probable que tenga éxito para tratamientos médicos, ya que ofrece identificación durante la duración del tratamiento y luego se desecha. Además se pueden usar para identificar/marcar células cancerosas o para guiar a robots quirúrgicos durante una operación. Sin embargo, las posibilidades ofrecidas por RFID, su bajo costo, facilidad de implantación y de lectura… parece que superan los beneficios de los tags celulares.

- *Tags UWB (Ultra Wide Band)*. La transmisión de señales simultáneamente en múltiples bandas de frecuencia pero emitiendo una potencia muy baja, dota a esta tecnología de un mayor rango de operación, menor consumo de energía y mayor robustez frente a interferencias. Sin embargo, el costo de este tipo de etiquetas es significativamente mayor.

- *Tags ópticos.* Requieren una precisa orientación para ser leídos, lo que los hace poco prácticos para la mayoría de las aplicaciones que consideramos. Su potencial ventaja es que permite proporcionar diferente información en función del ángulo de lectura. Esta característica puede ser de gran utilidad en aplicaciones de alta seguridad, en las que sólo

el ángulo adecuado asegura una correcta información. Su falsificación es realmente complicada. Además es posible combinar la información procedente de varios lectores para dotar de aún más seguridad a la información.

- *Tags de ADN.* Etiquetas que embeben pequeños fragmentos de ADN, para sistemas antirrobo y anti falsificación.

- *Tags de software.* Aunque la tecnología difiere significativamente en relación a las etiquetas RFID, su funcionalidad es muy similar. Se trata de una aplicación que permite asociar una determinada imagen o patrón (líneas/cuadros blancos/negros) a un enlace a Internet con información. Muy útil para acceder a gran cantidad de información relacionada con el objeto etiquetado.

Al estar estas tecnologías en un estado incipiente, no es posible realizar una comparación de los factores críticos como en casos anteriores.

3.7.2 RFID

Aunque sus características generales han sido vistas en profundidad anteriormente, a efectos de efectuar una adecuada comparación incluimos los aspectos considerados en las tecnologías consideradas anteriormente:

- *Posibilidad de modificar los datos*. Depende del estándar que se utilice, aunque sí es posible. Por ejemplo, utilizando el estándar EPC, existen básicamente varias clases de etiquetas: de sólo lectura, de una escritura y múltiples lecturas o de lectura escritura.

- *Seguridad de los datos*. En las últimas generaciones de dispositivos RFID es posible cifrar los datos, de forma que no puedan ser leídos con lectores RFID estándar.

- *Cantidad de datos almacenados*. Hasta 1 MB de información en los últimos prototipos.

- *Costos*. En descenso a medida que se aplican los últimos avances tecnológicos. El objetivo de hace unos años de alcanzar los 0,05 € por etiqueta parece cada vez más cercano, aunque lógicamente depende del tipo de etiqueta.

- *Estándares*. Existen diferentes estándares universalmente aceptados, y relacionados con la banda de frecuencia utilizada, que como ya hemos visto, determina el tipo de sistema RFID. Los dos estándares principales son el estándar EPC y el estándar ISO.

- *Vida útil*. Al no haber necesidad de contacto físico ni de baterías, la vida útil de las etiquetas pasivas es muy grande. Las etiquetas activas tienen limitada su vida útil a la duración de su batería.

- *Tamaño*. En general, desde el tamaño de un botón o un caramelo hasta el tamaño de un paquete de tabaco. No obstante, Hitachi® ha anunciado recientemente su muchip, un chip RFID con tecnología de 2,4 GHz y un tamaño de 0,4 x 0,4 mm, con un espesor de 0,06 mm.

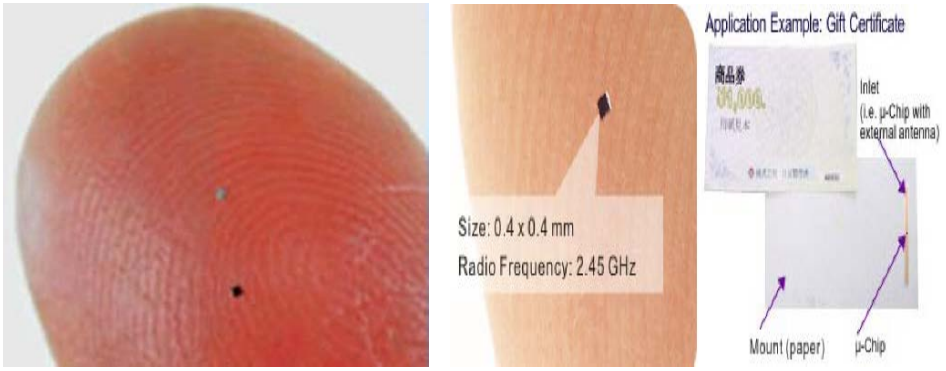


Figura 3.13. El mu-chip. Fuente: Hitachi.

- *Distancia de lectura*. Las etiquetas pasivas tienen un alcance del orden del metro, y las activas pueden tener un alcance de decenas de metros. Además, para realizar la lectura o escritura no se necesita línea de visión directa.
- *Número de elementos que se pueden leer simultáneamente*. Un lector puede leer cientos de etiquetas de forma casi simultánea.
- *Posibilidad de interferencias*. En función de la frecuencia, los líquidos, madera o metales puede impedir la propagación de la señales.

Por otro lado, si comparamos RFID con las tecnologías emergentes citadas, tenemos la siguiente tabla:

TECNOLOGIA	Principales ventajes frente a RFID	Principales desventajas frente a RFID
SAW	Costo sensiblemente inferior. Mejor funcionamiento en presencia de líquidos.	Etiqueta no modificable: una única escritura (en fabricación). Problema de colisiones entre lecturas aún no resuelto.
Tags Celulares	Baja vida útil, beneficio para determinadas aplicaciones.	Costo. Facilidad de lectura. Facilidad de implantación.
Tags UWB	Menor consumo de potencia. Mayor cobertura. Robustez frente a interferencias.	Costo muy superior.
Tags Ópticos	Costo inferior, (similar al código de barras). Elevada seguridad en la información contenida.	Poco práctica para las aplicaciones usuales.
Tags ADN	Elevada seguridad de la información.	Poco desarrollada aún.
Tags de Software	Almacena gran cantidad de Información. Útil para aplicaciones específicas.	Poco práctico para aplicaciones de inventariado. No válido para aplicaciones de localización/seguimiento.

Tabla 3.3 Comparativa de RFID con tecnologías competidoras emergentes.

Aunque RFID ha aparecido con fuerza, no debemos esperar que sustituya con rapidez a las tecnologías existentes. Al igual que tampoco hemos de esperar que aquellas tecnologías que vienen por detrás, sustituyan rápidamente a la tecnología RFID. Todas las tecnologías tienen sus fortalezas y debilidades y RFID no supone ninguna excepción. Sin embargo, no cabe duda que será necesaria una labor de monitorización y vigilancia de estas tecnologías para no verse sorprendidos por una solución tecnológica más barata y eficiente y que, sin darnos cuenta, ha entrado a formar parte del campo de aplicación o sector donde estamos trabajando con otra tecnología que a priori parecía óptima en ese entorno.

3.7.3 Near Field Communications (NFC)

La tecnología NFC (Comunicaciones en Campo Cercano) ofrece nuevas funcionalidades a la tecnología RFID propiamente dicha, gracias a la combinación de una etiqueta y un lector RFID en un mismo dispositivo. Este hecho facilita la comunicación bidireccional entre dos dispositivos, pudiendo actuar ambos como emisor y como receptor. La tecnología NFC rompe por tanto con la separación funcional descrita en apartados anteriores, entre el lector y la etiqueta RFID.

La tecnología NFC resulta especialmente útil aplicada a los dispositivos móviles (teléfonos, PDAs), de modo que el usuario lleva en su terminal móvil además de una etiqueta RFID con sus datos (o la información necesaria para cada aplicación), un lector para poder leer información de otras

etiquetas. De este modo se complementa la comunicación a corta, media y larga distancia provista por los dispositivos móviles (Bluetooth, WiFi, GPRS, UMTS) con la comunicación a muy corto alcance (centímetros) provista por NFC.

NFC surgió en el año 2002 como resultado de la cooperación entre Philips, Sony, y posteriormente Nokia. Se trata de un estándar ISO, ECMA y ETSI que trabaja en la banda de frecuencia HF (13.56MHz) y por tanto con un rango de cobertura pequeño (<10cm).
Actualmente ofrece velocidades de transmisión de datos de 106kbps, 212kbps y 424kbps - no está pensado para transmitir grandes volúmenes de datos, sino más bien para intercambiar información de forma rápida, eficiente y segura-. Al igual que el resto de tecnología RFID, el protocolo NFC cubre los modos de operación activo y pasivo.

El NFC Forum9 ha desarrollado cuatro tipos diferentes de etiquetas que todo dispositivo
NFC debe soportar:

- Tipo 1: basado en ISO 14443 A. Proporcionado por Innovation Research &Technology (TopazTM) 10. Posee una capacidad de hasta 1 Kbits y velocidades de transmisión de 106 Kbps Son etiquetas de bajo costo.
- Tipo 2: basado en ISO 14443 A. Proporcionado por NXP Semiconductors11 (MIFARE Ultra Light) 12. Posee una capacidad de 0.5 Kbits y velocidad similares a las tipo 1. También son de bajo costo.
- Tipo 3: basado en FeliCa13 (que deriva de ISO 18092). Proporcionado por Sony, con capacidades de hasta 2 Kbits y velocidades de 212 Kbps El costo es mayor aunque útil para aplicaciones más complejas.
- Tipo 4: Basado en ISO 14443 A/B. En este caso son varios fabricantes los que proporcionan este tipo de etiquetas. Posee capacidad de hasta 64 Kbits y velocidades comprendidas entre 106 Kbps y 424 Kbps

La elección del tipo de etiqueta a utilizar dependerá del tipo de aplicación que se necesite. NFC es especialmente útil en su aplicación a medios de pago, aunque también se está tratando de introducir en aplicaciones de transporte, de control de accesos o incluso en entornos sanitarios y de cuidados de la salud. Existen fundamentalmente tres tipos de aplicaciones que la tecnología NFC puede habilitar:

- Conexión P2P (Peer To Peer) entre dos dispositivos NFC. Facilita la transferencia de datos para la sincronización y autoconfiguración entre dos dispositivos, por ejemplo, en el momento de establecer una conexión posterior de más largo alcance o de mayores tasas de transferencia (Wifi, Bluetooth).

- Pagos y tickets. Facilita la realización de pagos electrónicos y la obtención de billetes de transporte de forma inteligente.
- Servicios de inicialización. Facilita el descubrimiento de servicios o el desbloqueo/lanzamiento de los mismos (por ejemplo, abrir una puerta o lanzar una aplicación).

En el ámbito de la salud, la tecnología NFC ofrece interesantes escenarios de aplicación, especialmente en la gestión de pacientes que sufren enfermedades crónicas y requieren una periódica monitorización. En este sentido, NFC ofrece a los pacientes la posibilidad de acceder a los sistemas de monitorización en el hogar. Los equipos de medida dotados de tecnología NFC se comunican con el móvil del paciente, que envía la información recogida al centro de salud. Este proceso de autogestión garantiza la provisión de un tratamiento adecuado y actualizable en tiempo real, en función de la evolución del paciente, cualidad especialmente útil en el caso de enfermedades crónicas.

Otra oportunidad significativa podría surgir en la atención a pacientes externos, permitiendo a los profesionales sanitarios atender a pacientes externos que se encuentran en sus domicilios. Lo mismo ocurre con las visitas domiciliarias, en los que el profesional que realiza la visita, puede leer la información del paciente y administrarle en consecuencias los servicios o tratamientos apropiados.

Por último el progreso e implantación de la receta electrónica permitirá realizar la compra de medicamentos directamente desde el teléfono móvil NFC.

El futuro de esta tecnología es aún incierto. Aunque actualmente existen algunas experiencias y pilotos al respecto, aún resultan insuficientes para mostrar al mercado las potencialidades de esta tecnología. Hoy en día, existen pruebas de esta tecnología incorporada a teléfonos móviles que se están utilizando comercialmente como medio de pago en Alemania y Austria, y como pilotos en Londres, Singapur, Holanda y Finlandia y Nueva York, entre otros. El futuro parece por tanto prometedor.

Finalmente el éxito de esta tecnología dependerá de la producción masiva de dispositivos móviles NFC (como el Nokia 6131 NFC), que aún resulta demasiado escasa. Pero no únicamente depende de la tecnología en sí, sino también de la estandarización e interoperabilidad que se logre alcanzar, y de la superación de los temas de seguridad y privacidad. Además, será necesario considerar la complejidad de las relaciones entre todos los actores del modelo de negocio: administración, operadoras de telefonía y el sistema bancario.

4. Tecnología

La Tecnología es una característica propia del ser humano consistente en la capacidad de éste para construir, a partir de materias primas, una gran variedad de objetos, máquinas y herramientas, así como el desarrollo y perfección en el modo de fabricarlos y emplearlos con vistas a modificar favorablemente el entorno o conseguir una vida más segura.
El ámbito de la Tecnología está comprendido entre la Ciencia y la Técnica propiamente dichas, Por tanto el término "tecnológico" equivale a "científico-técnico". El proceso tecnológico da respuesta a las necesidades humanas; para ello, recurre a los conocimientos científicos acumulados con el fin de aplicar los procedimientos técnicos necesarios que conduzcan a las soluciones óptimas. La Tecnología abarca, pues, tanto el proceso de creación como los resultados.

Por tal motivo el presente capitulo hace referencia a esos conocimientos científicos acumulados que han sido la base de referencia y existencia de la tecnología RFID.

Se empieza con los conceptos básicos pero fundamentales como son el espectro radioeléctrico, señal eléctrica y campo magnético, pasando por la región de propagación de ondas electromagnéticas hasta llegar a los métodos de acoplamiento usados en la RFID

4.1 Espectro Radioeléctrico

El fenómeno físico que aplica en el funcionamiento de las tecnologías de RFID es la transmisión y recepción de ondas electromagnéticas que contienen información del objeto a identificar. En la figura (4.1) se muestra un esquema del espectro radioeléctrico.

La tecnología RFID opera en las bandas de frecuencias bajas (LF), altas (HF), ultra altas (UHF), y súper altas (SF). Las longitudes de onda para las frecuencias bajas y altas son del orden de centímetros y para las frecuencias ultra y súper altas son en metros.

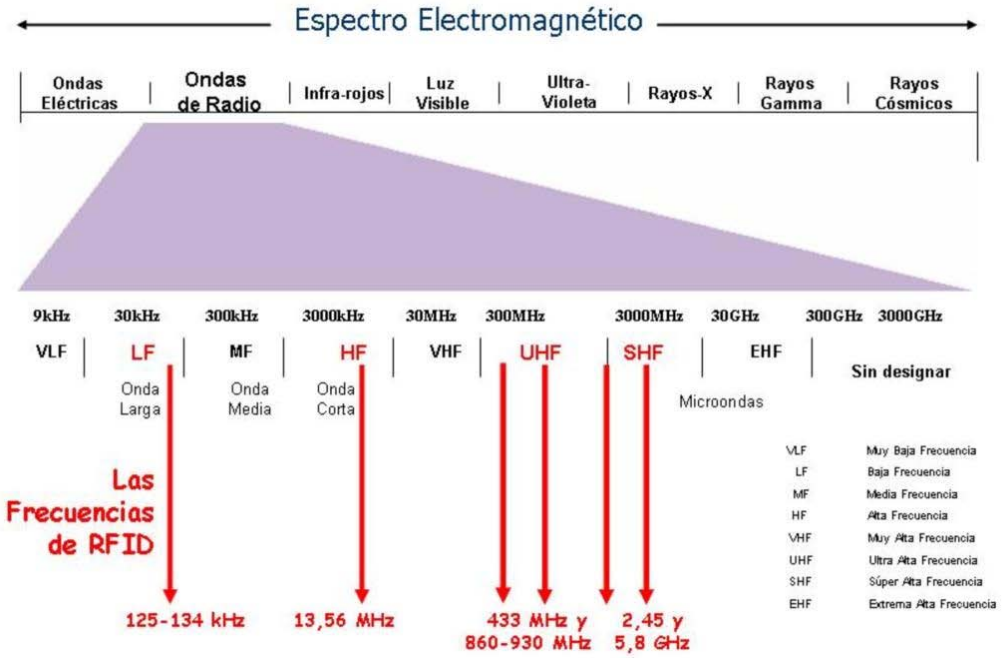


Figura 4.1 Representación del Espectro Electromagnético

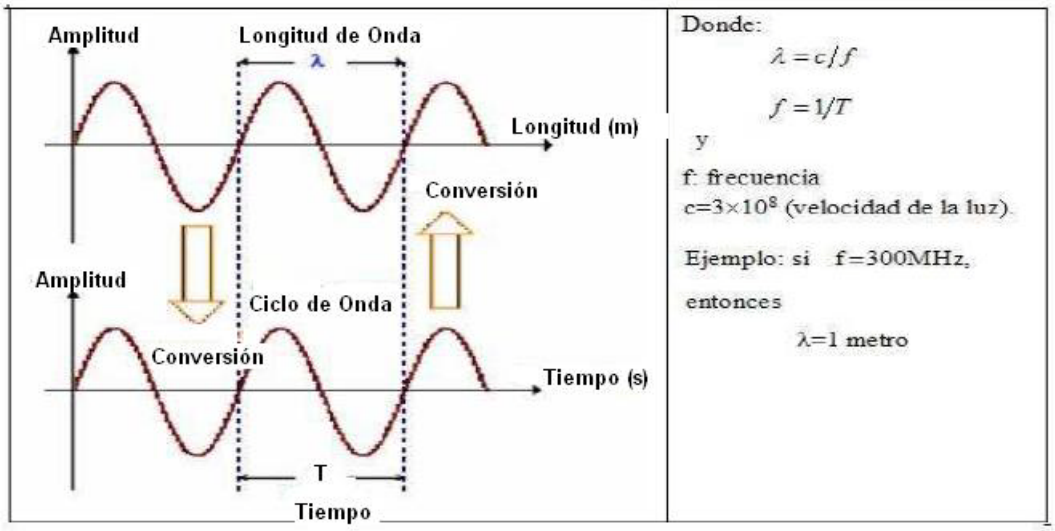


Fig. 4.2: Relación de la longitud de onda con la frecuencia

Señal Radioeléctrica

La onda radioeléctrica está compuesta por un campo eléctrico (E) y un campo magnético (H). Su propagación depende de la frecuencia y de las características eléctricas del medio, cuyo parámetro importante es la impedancia, que es la relación entre los campos mencionados.

La referencia de propagación es el espacio libre que tiene una impedancia igual a:

$$\eta_0 = [E/H] = 120[\Omega] \approx 377[\Omega] \qquad (4.1)$$

En la región del espacio libre el campo eléctrico viaja transversal al campo magnético y la onda se conoce como onda-plana. Una onda electromagnética transversal se muestra en la figura (4.3)

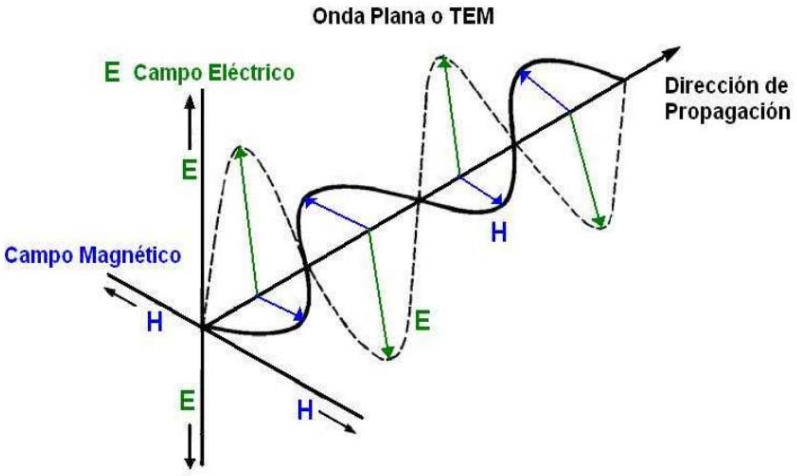


Figura 4.3. Onda Plana o electromagnética transversal

En la figura (4.4) se muestra la relación de la impedancia respecto a la onda plana para la región de campo cercano reactivo y campo lejano.

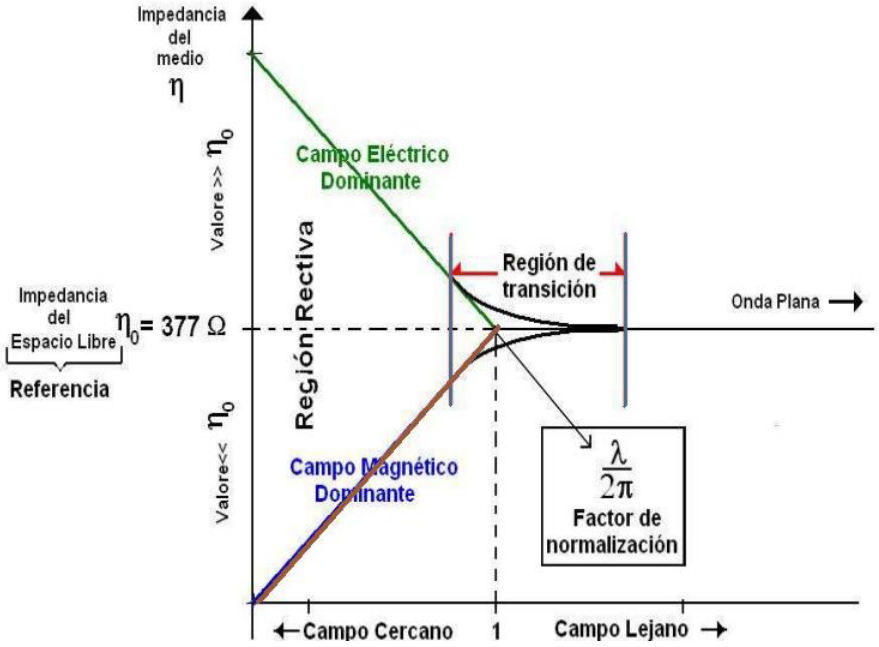


Figura 4.4 Relación de la impedancia respecto a la onda plana

El campo magnético H

Cada movimiento de carga se asocia con un campo magnético. La presencia de los campos magnéticos se demuestra, por ejemplo, en la creación de una corriente eléctrica secundaria. El campo magnético depende de las cargas que lo crean, del punto donde se estudia, y del medio donde se crea el campo. Pero experimentalmente se descubrió que existe una magnitud que no depende del medio donde se cree, esta magnitud del campo magnético se define como intensidad del campo magnético H. Se puede ver en (4.2) y (4.3) la relación con el campo magnético B, como es la relación entre el campo magnético y la corriente que circula, por ejemplo, por un conductor.

$$\vec{H} = \frac{\vec{B}}{\mu} \tag{4.2}$$

$$\sum I = \oint \vec{H} \cdot \vec{ds} \tag{4.3}$$

Podemos usar (4.2) para calcular el campo magnético para diferentes tipos de conductores, como los de la Figura 4.5.

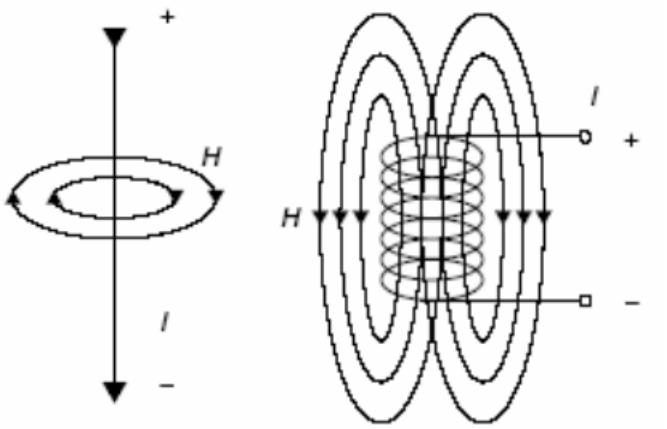


Figura 4.5 Líneas de flujo magnético alrededor de un hilo conductor y de una bobina.

El campo magnético se representa mediante líneas de fuerza, trazadas de modo que en cada uno de sus puntos el vector B es tangente.

Campo magnético H en espiras

Un aspecto importante para los diseños en la trayectoria que forma campo magnético (H) creado por una corriente que atraviesa unas espiras (conductor loop), también llamadas “short cylindrical coils”. Estas espiras son usadas como antenas generadoras de un campo magnético en diseños

de sistemas RFID con acoplamiento inductivo. Podemos ver en la Figura 4.6 las líneas de campo magnético en conductores cilíndricos. [19]

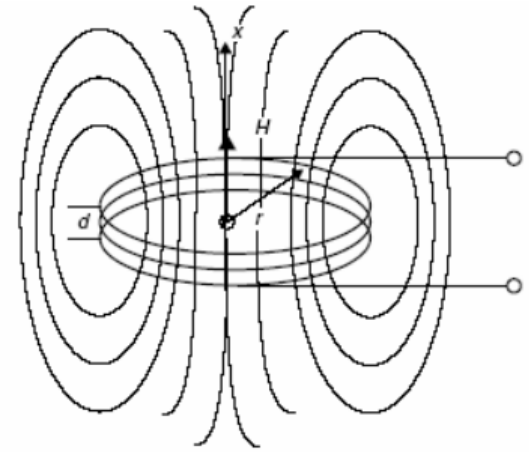


Figura 4.6 Las líneas de flujo magnético que alrededor de los conductores en espira son similares a las empleadas en las antenas transmisoras de los sistemas RFID de acoplamiento inductivo.

El campo magnético H decrece con la distancia en el eje x. También se sabe que el campo H en relación con el radio de la espira r, permanece constante a una cierta distancia, y comienza a decrecer rápidamente. La Figura 4.7 permite visualizar gráficamente estas relaciones.

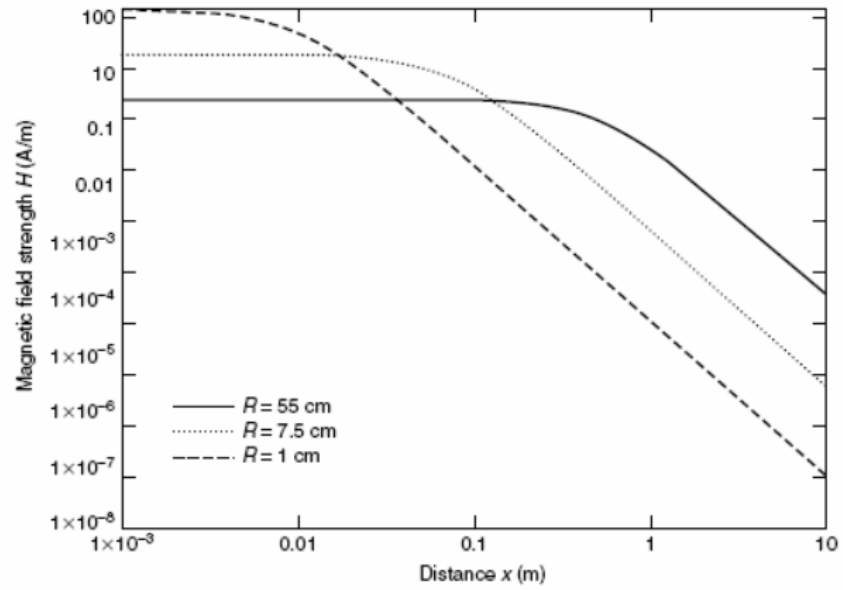


Figura 4.7 Intensidad del campo magnético H en relación con la distancia del centro de las espiras (eje x) y el radio de las espiras.

Para calcular el valor de H en el eje x usamos (4.4).

$$H = \frac{I \cdot N \cdot R^2}{2\sqrt{(R^2 + x^2)^3}} \qquad (4.4)$$

Donde N es el número de espiras, R es el radio de la espira y x la distancia desde el centro de la espira, en la dirección del eje x. Para estas ecuaciones se toman como aproximaciones d<<R y x<λ/2π.

Por otro lado tenemos que en centro de la espira, es decir, con x=0:

$$H = \frac{I \cdot N}{2R} \tag{4.5}$$

En general, para lo que nos afecta al diseño de antenas transmisoras de RFID, hemos de saber cuanto más grande es el radio de la espira que forman la antena, en los sistemas con acoplamiento inductivo, más fuerte es el campo magnético en distancias mayores que el radio, y en cambio cuando el radio es pequeño más fuerte es el campo en distancias menores al radio.

Por estos motivos, a la hora de diseñar un sistema RFID debemos elegir un diámetro de antena óptimo. Si elegimos un radio demasiado grande, si es cierto que tendremos un mayor alcance, pero el campo magnético cerca del centro de la espira (x=0) será muy débil, y por el contrario si elegimos un radio demasiado pequeño, nos encontraremos con un campo magnético que decrece en proporción de x3

Por tanto el radio óptimo de la antena de transmisión debe ser el doble del máximo alcance de lectura deseado.

En la práctica, aplicando estas teorías a los sistemas RFID, para conocer el alcance máximo de un lector, hay que saber también las características del campo magnético mínimo a recibir del transponder a leer. Si la antena seleccionada tiene un radio muy grande, entonces se corre el peligro que el campo magnético H pueda ser insuficiente para alimentar a los transponders que se encuentren más cerca de la antena del lector.

Flujo magnético y densidad del flujo magnético

El número total de líneas de campo magnético que pasan a través de una espira circular se conoce como flujo magnéticoΦ, definido en un área A y con una densidad de flujo magnético B como podemos ver en la Figura 4.8. La fórmula (4.6) representa esta relación.

$$\Phi = B \cdot A \tag{4.6}$$

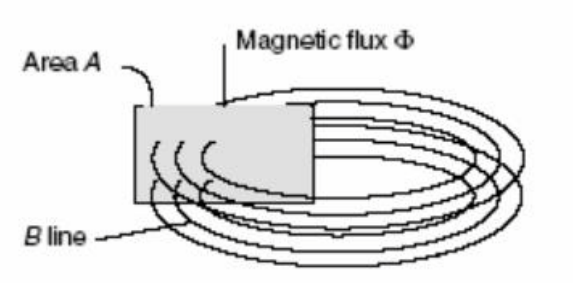


Figura 4.8 Relación entre el flujo magnético Φ y la densidad de flujo B.

La relación entre el campo magnético B y el campo magnético H se expresa según (4.7)

$$B = \mu_0 \mu_r H = \mu H \tag{7.7}$$

Donde la constante μo describe la conductividad magnética o permeabilidad en el vacío. La variable μr es la permeabilidad relativa e indica cuanto de grande o cuanto de pequeña es que μo dependiendo del material.

Inductancia L

Cualquier circuito es atravesado por un flujo creado por el mismo y que debe ser proporcional a la intensidad que lo recorre como vemos en (4.8). El flujo es particularmente elevado si el conductor tiene forma de espira. Normalmente hay más de una espira, N espiras en la misma área A, a través de las cuales circula la misma corriente. Cada espira contribuye con la misma proporciónΦ al flujo total Ψ, podemos ver la relación en (4.8).

$$\Psi = \sum_N \Phi_N = N \cdot \Phi = N \cdot \mu \cdot H \cdot A \tag{4.8}$$

Definimos como inductancia L, la relación entre el flujo total y la corriente que atraviesa el conductor.

$$L = \frac{\Psi}{I} = \frac{N \cdot \Phi}{I} = \frac{N \cdot \mu \cdot H \cdot A}{I} \tag{4.9}$$

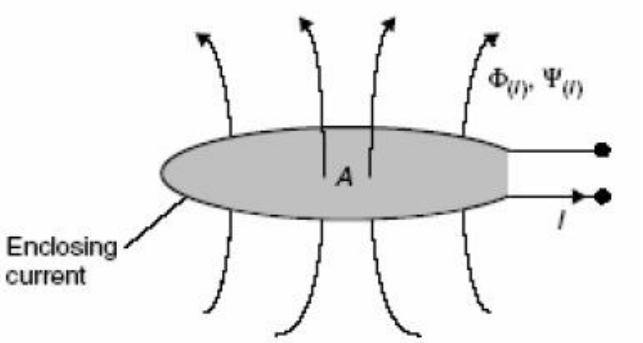


Figura 4.9 Definición de Inductancia L

La inductancia es una de las características variables de este tipo de conductores. La inductancia de los conductores en espira depende totalmente de las propiedades del material (permeabilidad) que la atraviesa el flujo del campo magnético y de la geometría del layout.

Si suponemos que el diámetro d del conductor usado es muy pequeño comparado con el diámetro D de la espira del conductor (d/D<0.0001), podemos realizar la aproximación (4.10):

$$L = N^2 \mu_0 R \cdot \ln\left(\frac{2R}{d}\right) \tag{4.10}$$

Dónde R es el radio de la espira del conductor y d el diámetro del conductor usado.

Inductancia Mutua M

La inductancia mutua se produce por la proximidad de dos conductores en forma de espira. La corriente que atraviesa una de las espiras induce un flujo magnético en el otro y al inverso. La magnitud del flujo inducido depende de las dimensiones geométricas de ambos conductores, la posición de un conductor respecto al otro y las propiedades magnéticas del medio. Para dos conductores de áreas A1 y A2, e I1 la corriente que circula por la primera espira vemos:

$$M_{21} = \frac{\Psi_{21}(I_1)}{I_1} = \oint_{A2} \frac{B_2(I_1)}{I_1} \cdot dA_2 \tag{4.11}$$

Por definición tenemos que la inductancia mutua es igual:

$$M = M_{12} = M_{21} \tag{4.12}$$

La inductancia mutua siempre esta presente entre dos circuitos electrónicos, en este principio físico es en el que se basa el acoplamiento inductivo de los sistemas RFID.

En la Figura 4.10 podemos ver la definición de inductancia mutua por dos espiras.

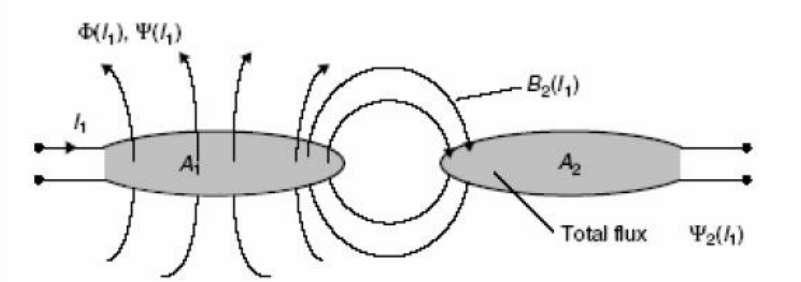


Figura 4.10 Inductancia mutua por dos espiras.

Si aplicamos (4.13) a dos espiras:

$$M_{12} = \frac{\mu_0 \cdot N_1 \cdot R_1^2 \cdot N_2 \cdot R_2^2 \cdot \pi}{2\sqrt{(R_1^2 + x^2)^3}} \qquad M_{12} = \frac{B_2(I_1) \cdot N_2 \cdot A_2}{I_1} = \frac{\mu_0 \cdot H(I_1) \cdot N_2 \cdot A_2}{I_1} \tag{4.13}$$

Coeficiente de acoplamiento k

Si la inductancia mutua describía cualitativamente el flujo creado por la corriente que circula por otra espira, el coeficiente de acoplamiento realiza una predicción cualitativa de la inducción creada entre dos espiras independientemente de las dimensiones geométricas de los conductores.

$$k = \frac{M}{\sqrt{L_1 \cdot L_2}} \tag{4.14}$$

Tenemos que 0≤k≤1, por lo que en los casos extremos:

k=0: No hay acoplamiento debido a la gran distancia no hay acción del campo magnético.

k=1: Acoplamiento total. Las dos espiras están sometidas al mismo Φ. El transformador es la aplicación técnica con total acoplamiento.

Resonancia

El voltaje inducido u2 en la antena del transponder es usado como alimentación necesaria para el chip en su proceso de almacenamiento de datos en memoria. Para mejorar la eficiencia un capacitador C2 se conecta en paralelo con la bobina del transponder L2, como vemos en la Figura 4.11, de manera que forma un circuito paralelo resonante con una frecuencia resonante que es la frecuencia de operación del sistema de RFID. La frecuencia resonante se puede calcular en (4.15).

$$f = \frac{1}{2\pi\sqrt{L_2 \cdot C_2}} \tag{4.15}$$

En la práctica existe un capacitador parásito en paralelo Cp por lo que el valor del capacitador seria C_2, como vemos en (4.16).

$$C_2' = \frac{1}{(2\pi f)^2 L_2} - C_p \tag{4.16}$$

En la Figura 4.17 podemos ver el circuito equivalente de un transponder real, donde R_2 es la resistencia natural de la bobina del transponder L_2 y el consumo de corriente del chip viene dado por la resistencia de carga R_L

.

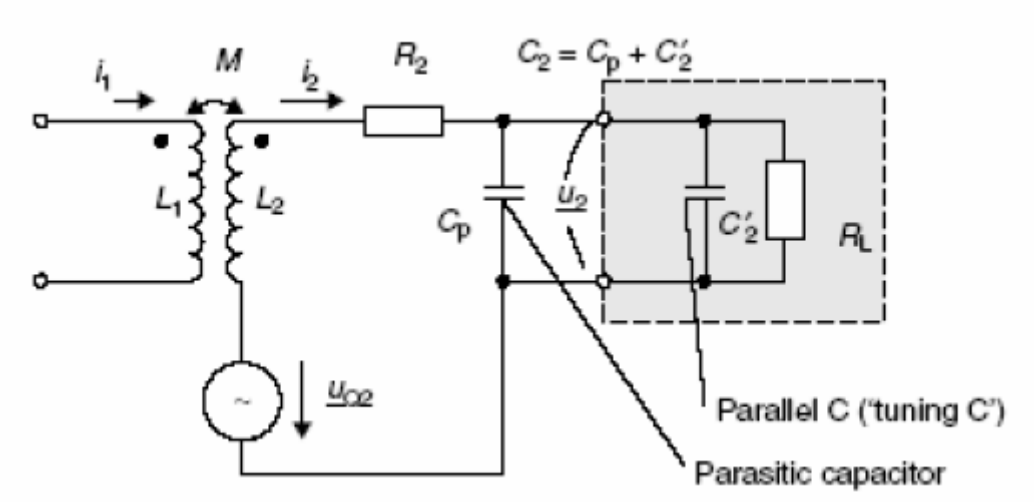


Figura 4.11 Diagrama del circuito equivalente para el acoplamiento magnético de dos bobinas. La bobina L_2 y el condensador en paralelo C2 forman el circuito resonante.

Cuando la frecuencia de operación es igual a la frecuencia de resonancia d circuito tenemos el mayor voltaje en la resistencia R_L

Se introduce el factor Q para comprobar cómo influyen los componentes del circuito R_L, R_2 y L_2 en el voltaje U_2. El factor Q es sencillo de calcular, (4.17), en este caso ω es la frecuencia angular, y es igual a 2πf en el circuito resonante.

$$Q = \frac{1}{R_2 \cdot \sqrt{\frac{C_2}{L_2}} + \frac{1}{R_L} \cdot \sqrt{\frac{L_2}{C_2}}} = \frac{1}{\frac{R_2}{\omega L_2} + \frac{\omega L_2}{R_L}} \qquad (4.17)$$

El voltaje U_2 es proporcional a la calidad del circuito resonante, lo que quiere decir que depende de R_2 y R_L. Por tanto a la hora de diseñar el transponder tendremos en cuenta estos parámetros y escogerlos para optimizar el rango de alcance del sistema.

4.2 Región de Propagación

Como en el mundo real no todo es espacio libre, se tienen definidas tres regiones donde pueden propagarse los campos electromagnéticos:

- Región de campo cercano reactivo. En esta región se tiene un campo dominante, puede ser magnético (fenómeno inductivo) o el eléctrico (fenómeno capacitivo), por lo que la transmisión se presenta como acoplamiento electromagnético.
- Región de campo cercano radiado. Después de la región de campo cercano reactivo las ondas electromagnéticas empiezan a radiarse generando círculos cerrados alrededor del elemento que genera el campo que es conocido como elemento radiador o antena. A esta región también se le conoce como zona de Fresnel.
- Región de campo lejano radiado. Esta región corresponde al espacio libre y es la referencia para analizar los fenómenos de propagación de ondas electromagnéticas.

  A continuación se muestra un esquema que ilustra las tres regiones antes mencionadas.

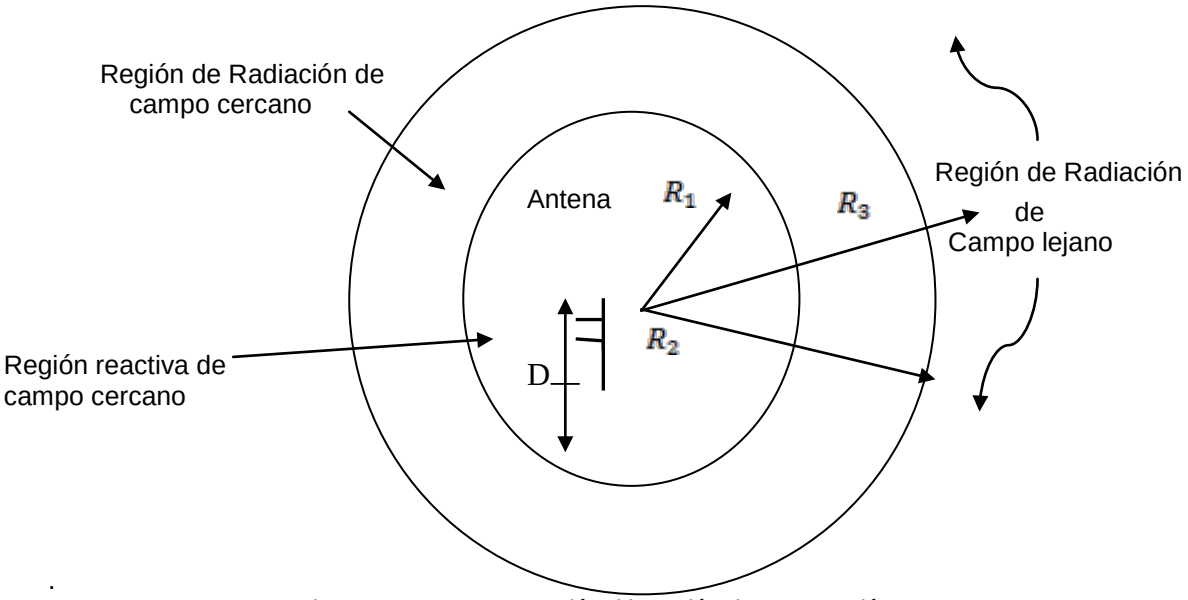


Figura 4.12. Representación d la región de propagación

Para transmitir información por medio de ondas electromagnéticas se requiere de dispositivos que se llaman antenas, convierten la energía electromagnética en energía eléctrica y operan de forma bidireccional, es decir una antena puede usarse como transmisora o receptora.

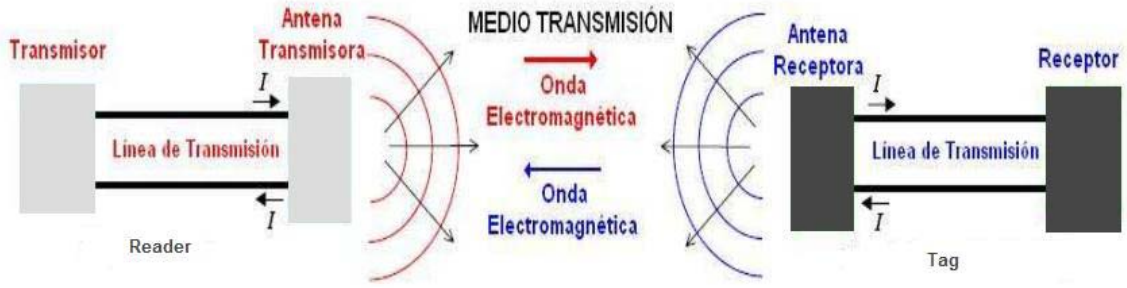


Figura 4.13 Representación de la transmisión en un sistema RFID

Para que la transmisión de la información tenga éxito, los sistemas deben trabajar a la misma frecuencia. Para la propagación de ondas en el espacio libre, las dimensiones de las antenas se especifican normalmente en fracciones de longitudes de onda (longitud eléctrica), valor típico es media longitud de onda (λ/2) o un cuarto de longitud de onda (λ/4). De acuerdo con esta consideración, la tecnología RFID que opera en la banda de LF, (125 KHz) tiene una longitud de onda de 2400m ($\lambda = 3 * 10^8 / 125 * 10^3$), entonces la antena que debe utilizarse para la transmisión de onda plana, debe ser de 1200m para λ/2 o 600m para λ/4 . Las antenas tienen dimensiones desproporcionadas para la aplicación de la tecnología de RFID. Estas frecuencias se pueden utilizar si las frecuencias operan bajo el esquema de campo cercano donde se presenta el

fenómeno de acoplamiento electromagnético, teniendo distancias de centímetros entre el emisor-receptor. Así mismo la tecnología que opera en las frecuencias HF, que tiene una longitud de onda de 22,123m, también funciona bajo el esquema de acoplamiento electromagnético. Para la frecuencia de operación de la tecnología RFID en la banda de UHF de 433 MHz la longitud de onda es $\lambda = 0{,}692m$ y para 915 MHz la longitud de onda es $\lambda = 0{,}33m$; para la banda de SHF de 2.45 GHz la longitud de onda es $\lambda = 0{,}122m$ y para 5.8 GHz la longitud de onda es $\lambda = 0{,}0517m$. En estas dos bandas si se puede operar en la región de campo lejano, ya que las antenas son de dimensiones adecuadas a la aplicación de la tecnología RFID.

4.3 Funcionamiento de los transponders

Ya hemos tratado el tema de la alimentación en los transponders, por lo que teníamos transponders activos que incorporaban su propia batería que era la encargada de alimentar el chip en su proceso de lectura/escritura; mientras que los transponder pasivos eran únicamente alimentados con el voltaje U_2, comentado anteriormente.

El voltaje inducido U_2 en la antena del transponder alcanza rápidamente valores elevados. Este voltaje hay que regularlo, para ello, independientemente de los valores del coeficiente de acoplamiento k o de otros parámetros, se utiliza el resistor R_s conectado en paralelo con la resistencia de carga R_L. Podemos ver el circuito equivalente en la Figura 4.14.

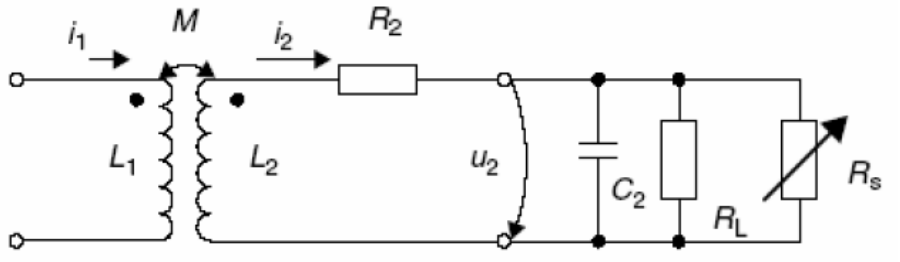


Figura 4.14 Regulador del voltaje en el transponder.

La tensión incrementa en medida que el valor de RS disminuye.

En el proceso de funcionamiento del transponder tenemos el valor del campo de interrogación del transponder,H_{min}.Es la mínima intensidad de campo (a la máxima distancia entre transponder y el reader) a la cual el voltaje inducido U_2 es justo el suficiente para realizar las operaciones del chip.

Para el cálculo de H_{min} tenemos (4.18), donde N es el número de espiras de la bobina L_2, y A es la sección de la bobina.

$$H_{\min} = \frac{u_2 \cdot \sqrt{\left(\frac{\omega L_2}{R_L} + \omega R_2 C_2\right)^2 + \left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)^2}}{\omega \cdot \mu_0 \cdot A \cdot N} \tag{4.18}$$

En (4.20) vemos que el campo de interrogación depende de la frecuencia por medio del factor ω=2πf y del área A de la antena, del número de espiras N de la bobina, del mínimo voltaje U_2 y de la resistencia de entrada R_2. Por eso cuando la frecuencia de transmisión del lector corresponde con la frecuencia de resonancia del transponder, el campo de interrogación mínimo H_{min} tiene su valor mínimo.

Para optimizar la sensibilidad de un sistema RFID con acoplamiento inductivo, la frecuencia de resonancia del transponder debe ser precisamente la frecuencia de resonancia del lector. Desafortunadamente esto no es siempre posible en la práctica.

Primero en la fabricación del transponder puede haber tolerancias, las cuales pueden provocar una desviación en la frecuencia de resonancia. Segundo, por razones técnicas a la hora de configurar la frecuencia de resonancia del transponder hay procedimientos que pueden diferenciarla de la frecuencia de transmisión del lector (por ejemplo en sistemas que usan procedimientos de anticolisión para que dos transponders no se estorben a la hora de comunicar datos).
En la ecuación (4.19) la frecuencia de resonancia es calculada como el producto de L_2C_2.

$$L_2C_2 = \frac{1}{(2\pi\ f_0)^2} = \frac{1}{\omega_0^2} \tag{4.19}$$

Si lo substituimos en (4.22) encontramos la dependencia de H_{min} con la frecuencia del lector (ω) y la frecuencia de resonancia del transponder (ωo). Se basa en el supuesto que la variación en la frecuencia de resonancia del transponder esta causada por la variación de C_2.

$$H_{\min} = \frac{u_2 \cdot \sqrt{\omega^2 \left(\frac{L_2}{R_L} + \frac{R_2}{\omega_0^2 L_2}\right)^2 + \left(\frac{\omega_0^2 - \omega^2}{\omega_0^2} + \frac{R_2}{R_L}\right)^2}}{\omega\mu_0 \cdot A \cdot N} \tag{4.20}$$

Si se conoce H_{min}, entonces se puede conocer el rango de energía asociado a ese rango de alcance del lector. El rango de energía del transponder es la distancia desde la antena del lector a la cual la energía para que opere el transponder es justo la suficiente (definido como U_2 en R_L), lo vemos en (4.21). El resultado de la pregunta de si el rango de energía es el igual al máximo

alcance funcional que tiene el sistema depende de si la transmisión de datos desde el transponder puede ser detectado por el lector a esa distancia en cuestión.

$$x = \sqrt{\sqrt[3]{\left(\frac{I \cdot N_1 \cdot R^2}{2 \cdot H_{\min}}\right)^2} - R^2} \qquad (4.21)$$

En (4.23) tenemos I como la corriente que circula por la antena, R el radio de las espiras y el número de espiras de la antena transmisora como N.

Se puedes decir que cuando incrementa el consumo de corriente, una RL más pequeña, la sensibilidad del lector se incrementa, por lo que el rango de energía decrece.

Durante todas las explicaciones hemos considerado un campo H homogéneo paralelo al eje de la bobina x. Por ejemplo la tensión inducida por un campo magnético en un ánguloθ viene dada (4.22).

$$u_{0\vartheta} = u_0 \cdot \cos(\vartheta) \qquad (4.22)$$

Donde U_0es el voltaje inducido cuando la espira es perpendicular al campo magnético, mientras que cuando el ángulo formado es de 90º no hay voltaje inducido en la espira. Podemos ver un ejemplo en la Figura 4.15 de las diferentes zonas alrededor de los lectores. Por eso, los transponders orientados en el eje x de la bobina obtienen un rango de lectura óptimo.

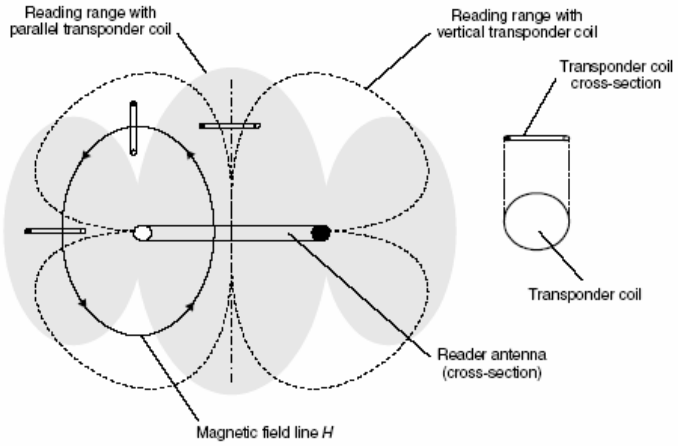


Figura 4.15 Zonas de interrogación del lector para diferentes alineamientos del transponder

Sistema transponder-reader

En este punto consideraremos las características de los sistemas con acoplamiento inductivo desde el punto de vista del transponder.

En la Figura 4.16 podemos ver el diagrama del circuito de un lector. La bobina necesaria para generar el campo magnético L_1. El resistor en serie R_1 corresponde con las pérdidas resistivas de las espiras de la bobina. Para obtener la máxima corriente en la bobina a la frecuencia de operación del reader f_{TX}, se crea el circuito resonante en serie con la frecuencia de resonancia $fRES$ =f_{TX}, con la conexión en serie del capacitador C_1. Se calcula con (4.23).

$$f_{TX} = f_{RES} = \frac{1}{2\pi\sqrt{L_1 \cdot C_1}} \tag{4.23}$$

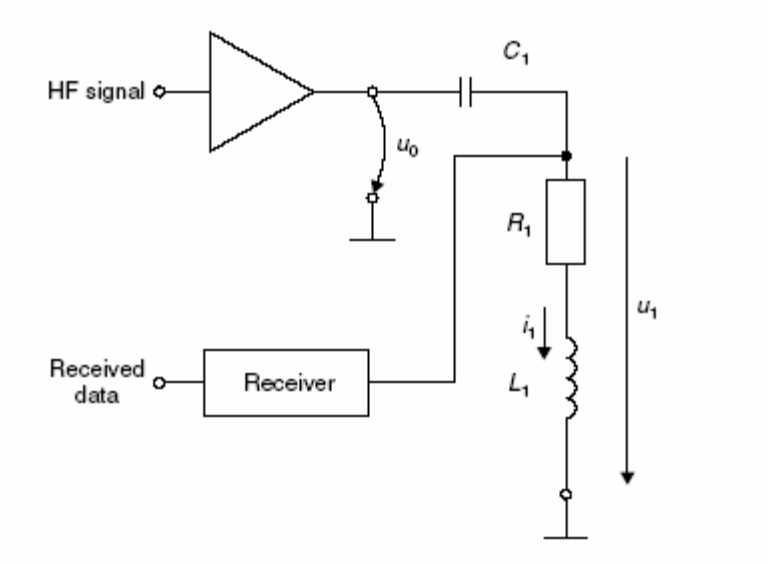


Figura 4.16 Diagrama del circuito equivalente de un lector RFID

Ondas Electromagnéticas

Como ya hemos visto una variación del campo magnético induce un campo eléctrico con líneas de campo cerradas.

Como el campo magnético propaga un campo eléctrico, éste originalmente puramente magnético se va transformando en un campo electromagnético. Además a la distancia de λ/2π el campo electromagnético comienza a separarse de la antena y comienza a desplazarse por el espacio en forma de onda electromagnético, podemos ver como se crea una onda electromagnética en la Figura 4.17

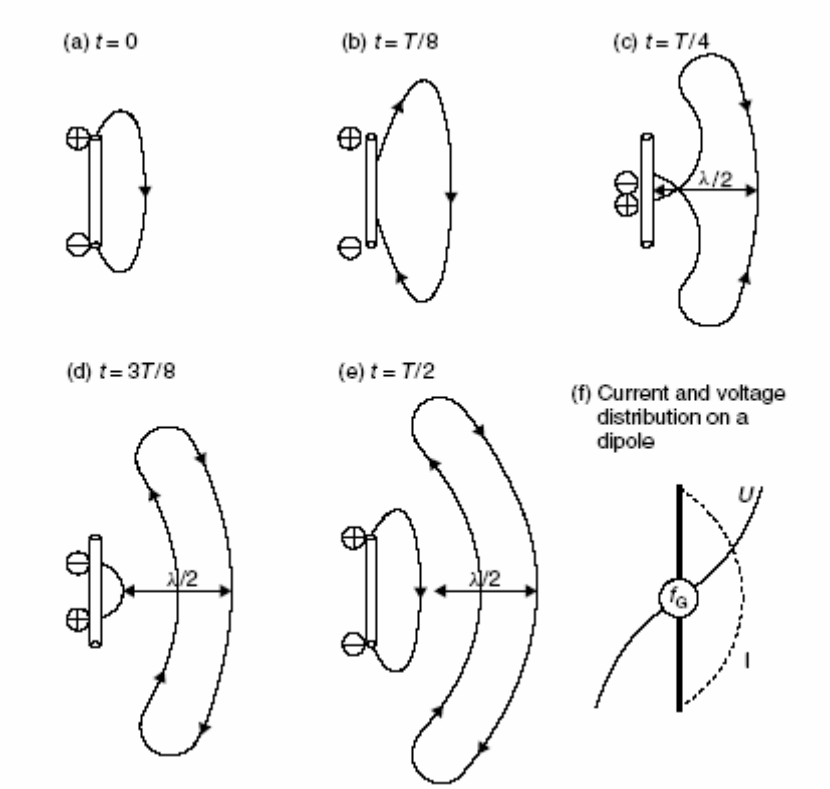


Figura 4.17 Creación de una onda electromagnética en un dipolo. El campo magnético forma un anillo alrededor de la antena.

El área desde la antena hasta el punto donde se forma la antena se conoce como "near field" de la antena, y el área a partir del punto donde se forma completamente la onda electromagnética se conoce como "far field".

Esto permite que el alcance de los sistemas por ondas electromagnéticas sea mayor que el producido por acoplamiento inductivo o capacitivo, que suelen representar su rango límite al principio del "far field". En la Figura 4.18 podemos observar como en el "near field" el campo magnético decrece en función de $1/d^3$ mientras que en el "far field" sólo decrece en función de 1/d

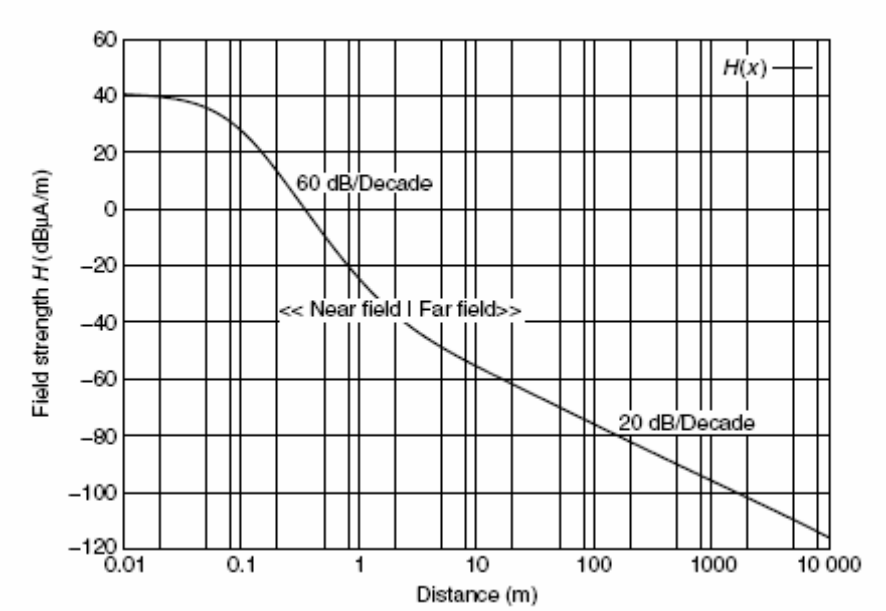


Figura 4.18 Gráfico de la intensidad de campo magnético en la transición de near y far field a la frecuencia de 13,56 MHz.

Densidad de Radiación

Una onda electromagnética se desplaza en el espacio esféricamente desde su punto de creación. Al mismo tiempo, las ondas electromagnéticas transportan energía. A medida que nos alejamos de la fuente de radiación, la energía es divida en el área de la superficie esférica que forma que se va incrementando. Aquí se introduce el término de densidad de radiación S.

En un emisor esférico, llamado isotrópico, la energía es radiada uniformemente en todas las direcciones. A la distancia r la densidad de radiación S puede calcularse fácilmente en (4.24) como el cuociente de la energía emitida P_{EIRP} (transmisor isotrópico) por el emisor y el área de la superficie de la esfera.

$$S = \frac{P_{\mathrm{EIRP}}}{4\pi r^2} \tag{4.24}$$

La energía transportada por las ondas electromagnéticas se almacena en los campos eléctrico y magnético de la onda. La relación entre los campos E y H y la densidad de radiación lo vemos en (4.25).

$$S = E \times H \tag{4.25}$$

En el vacío podemos aproximar la relación entre E y H como vemos en (4.26).

$$E = H \cdot \sqrt{\mu_0 \varepsilon_0} = H \cdot Z_{\mathrm{F}} \tag{4.26}$$

En la Figura 4.19 vemos el vector S como producto de E y H.

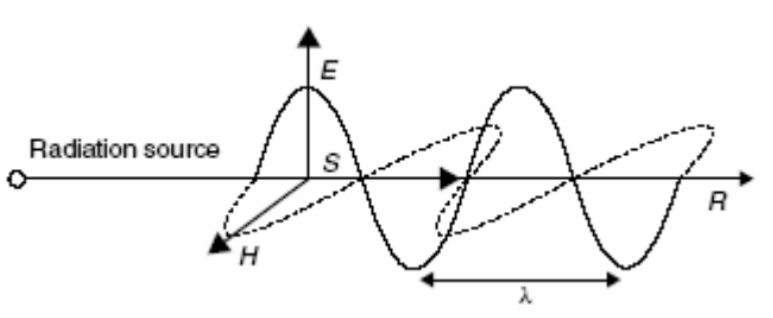


Figura 4.19 Vector S

Polarización

La polarización de una onda electromagnética se determina por la dirección del campo eléctrico de la onda. En la Figura 4.20 podemos diferenciar entre los diferentes tipos de polarizaciones.

Diferenciamos primero entre polarización lineal, donde también se diferencia entre polarización vertical y horizontal. Las líneas de campo eléctrico se desplazan en paralelo o perpendicular a la superficie terrestre. La transmisión de energía entre dos antenas linealmente polarizadas es máximo cuando las dos antenas están polarizas en la misma dirección, y mínima cuando forman un ángulo de 90º o 270º.

En los sistemas RFID no se puede conocer cual será la orientación entre la antena del transponder y la del lector. El problema es solucionado por el uso de la polarización circular del lector de la antena. El principio de generación de polarización circular se ve en la Figura 4.20, dos dipolos son unidos en forma de cruz. De esta forma el campo electromagnético generado rota 360º cada vez que se mueve el frente de onda una longitud de onda. Se diferencia por el sentido de giro del frente de onda izquierdas o derecha.

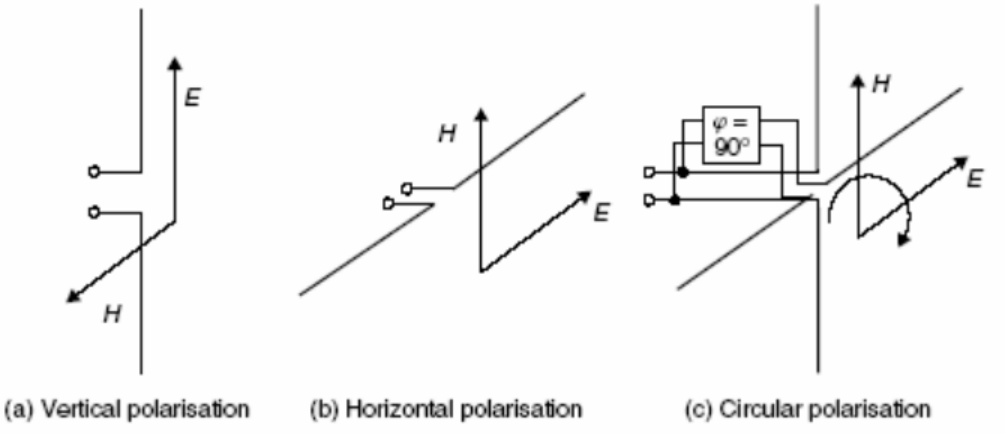


Figura 4.20 Definición de la polarización de ondas electromagnéticas.

Reflexión en ondas electromagnéticas

Una pequeña parte de la energía reflejada en objetos es devuelta a la antena transmisora. Es la tecnología en que se basa el radar para calcular la distancia y posición del objeto. En los sistemas de RFID la reflexión de las ondas electromagnéticas (sistema backscatter) es usada para la transmisión del transponder al lector. Las propiedades de la reflexión se hacen más notorias cuando se incrementa la frecuencia. La potencia de la onda reflejada decrece en proporción a r^2
Los sistemas backscatters emplean antenas con diferentes áreas de reflexión, llamado cross-section, que depende de varios factores como son el tamaño del objeto, el material, la estructura de la superficie, la longitud de onda (λ) y la polarización.

4.4 Funcionamiento de las Antenas

La elección de la antena es uno de los principales parámetros de diseño de un sistema RFID.

Definimos P_{EIRP} como la potencia emitida por un emisor isotrópico, y la podemos obtener en (4.27).

$$P_{\mathrm{EIRP}} = \int_{A_{\mathrm{sphere}}} S \cdot \mathrm{d}A \tag{4.27}$$

Aunque una antena real difiere de una isotrópica en que no radia uniformemente en todas las direcciones. Incluimos el término de ganancia (Gi) para una antena como la dirección de máxima radiación, indicando el factor por el cual la densidad de radiación es mayor que la de un emisor isotrópico con la misma potencia de transmisión. Si P_1 es la potencia emitida por la antena. Así definimos también en (4.28) P_{EIRP}. Vemos estos factores en la Figura 4.21

$$P_{\mathrm{EIRP}} = P_1 \cdot G_{\mathrm{i}} \tag{4.28}$$

Un emisor isotrópico tiene una ganancia igual a 1.

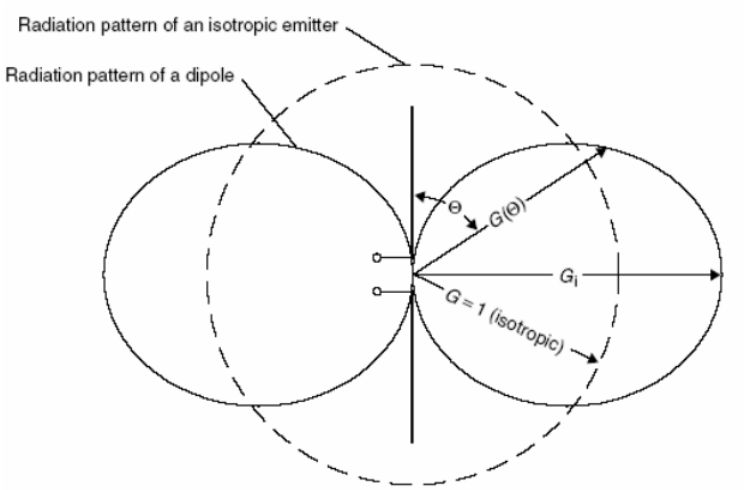


Figura 4.21 Comparación entre la radiación de un dipolo y un emisor isotrópico.

Podemos diferenciar entre EIRP o ERP, mientras EIRP como comentábamos es la potencia emitida por una antena isotrópica, EIR es la emitida por un antena dipolo. Y están relacionadas por (4.29).

$$P_{\text{EIRP}} = P_{\text{ERP}} \cdot 1.64 \tag{4.29}$$

Si nos centramos en el tipo de antenas de dipolos, las utilizadas en nuestro diseño, vemos que consiste en una sola línea de cobre. La antena más utilizada el dipolo λ/2, consiste en una línea de longitud l= λ/2, la cual está cortada a mitad, que es por donde se alimenta. Vemos en la tabla 4.1 las principales características de los dipolos λ/2.

Parameter	Gain G	Effective aperture	Effective length	Apex angle
λ/2 dipole	1.64	$0.13\,\lambda^2$	$0.32\,\lambda$	78°
λ/2 2-wire folded dipole	1.64	$0.13\,\lambda^2$	$0.64\,\lambda$	78°

Tabla 4.1 Propiedades eléctricas del dipolo y el doble dipolo λ/2.

4.5 Funcionamiento de los transponders de microondas

Nos centramos en el funcionamiento del transponder cuando se encuentra en el rango de alcance del lector. La Figura 4.22 muestra el modelo simplificado de un sistema backscatter.

El lector emite una onda electromagnética con una potencia efectiva de $P_1 \cdot G_1$ y el transponder recibe una potencia proporcional P_s al campo E y a la distancia r. La potencia P_s es la reflejada por la antena del transponder y la potencia P_3 es recibida por el lector a una distancia r.

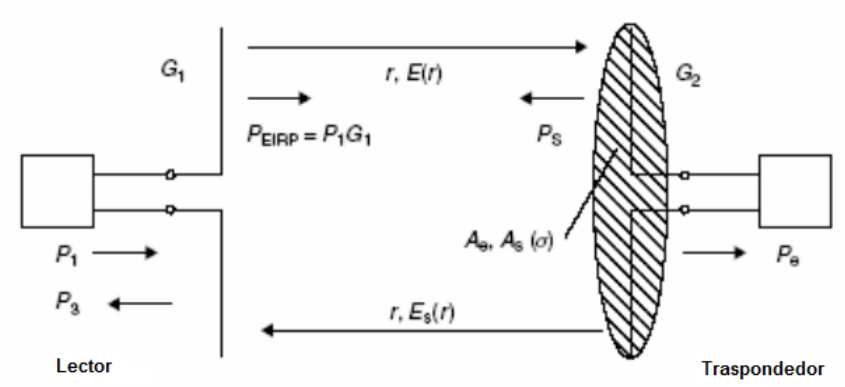


Figura 4.22 Modelo de sistema RFID por microondas cuando el transponder está en la zona de interrogación del lector.

Sensibilidad del transponder

A pesar del tipo de alimentación que tenga el transponder, activa o pasiva, un mínimo campo eléctrico es necesario para activar el transponder o alimentar con suficiente energía para que opere el circuito. La mínima intensidad de campo E_{min}se calcula fácilmente (4.30).

$$E_{\min} = \sqrt{\frac{4\pi \cdot Z_F \cdot P_{e\text{-}\min}}{\lambda_0^2 \cdot G}} \qquad (4.30)$$

En esta ecuación tenemos a Z_F como impedancia de entrada y la P_{e-min} como la potencia mínima requerida. Esto está basado en el requisito que las direcciones de polarización de las antenas del lector y del transponder correspondan. De otro modo el E_{min} incrementaría.

Rango de lectura

Para la comunicación entre el lector y el transponder se deben cumplir dos condiciones. Primero el transponder debe estar suficientemente alimentado para su activación y la señal reflejada por el transponder debe ser lo suficientemente potente para que cuando la reciba el lector la pueda detectar sin errores.

En los lectores backscatter la permanente transmisión, la cual es requerida para activar el transponder, introduce un ruido significativo, que reduce la sensibilidad del receptor del lector. Se puede asumir en la práctica que para que el transponder sea detectado, la señal del transponder no debe ser inferior a 100 dB por debajo del nivel de transmisión del lector. Para la transmisión de datos reflejados por el transporte se usan modulaciones. La potencia P_s reflejada se modula en una señal portadora y dos bandas laterales. La señal portadora no contiene información, pero es necesaria. En una modulación pura ASK las dos bandas laterales contienen el 25% del total de la potencia reflejadaP_s

Podemos ver una representación de los niveles de estas bandas laterales en la Figura 4.23.

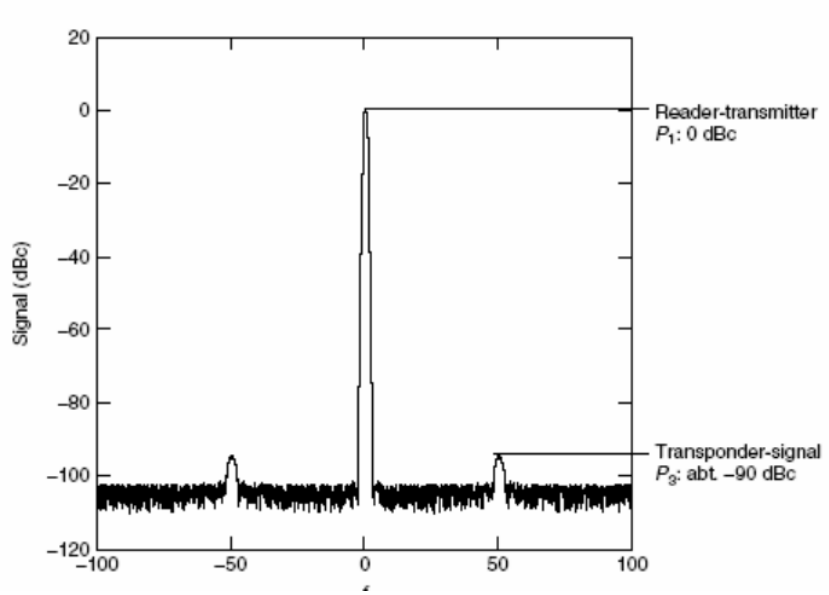


Figura 4.23 Niveles en el lector, podemos ver la señal propia del lector y las bandas laterales que provienen del transponder.

Podemos obtener la potencia de la onda que transmite el transponder al lector. (4.31).

$$P_3 = \frac{P_1 \cdot G_{\text{Reader}}^2 \cdot \lambda_0^4 \cdot G_{\text{T}}^2}{(4\pi r)^4} \tag{4.31}$$

El valor de la P_3 representa la potencia total reflejada por el transponder.

4.6 Procesamiento de comunicación en un solo sentido HALF DU- PLEX o ambos sentidos FULL DUPLEX

A diferencia de los sistemas de 1 bit en el transponder, guardado por efectos físicos, este tipo de sistemas utilizan un microchip electrónico como dispositivo portador de la información, el cual consta de una capacidad de almacenamiento de datos de unos cuantos kbytes. Para poder leer o escribir en dicho dispositivo es necesario establecer una comunicación entre el lector y el dispositivo, esta puede llevarse a cabo por medio de transmisión por *HALF DUPLEX (HDX)* o *FULL DUPLEX (FDX)*.

En el primero (HDX), el dato transferido desde el transponder se alterna con el dato transmitido desde el lector al transponder. Esto se realiza en frecuencias por debajo de los 30 MHz ya sea con una modulación con subportadora o sin subportadora. Para Full Dúplex (FDX) el dato transferido

desde el transponder al lector se efectúa simultáneamente a la transmisión del dato del lector al transponder.

En el caso de los sistemas secuenciales tenemos la transferencia de energía en un periodo limitado de tiempo, mientras que la transferencia de datos desde el transponder al lector ocurre en las pausas producidas por el lector.

4.7 Códificación

En el diagrama de bloques de la Figura 4.24 vemos descrito un sistema de comunicación digital. Similarmente, la transferencia de datos entre al el lector y la etiqueta en un sistema RFID requiere 3 bloques básicos de funcionamiento.

Desde el lector hacia el tag (dirección de la transferencia de datos) son:

- En el lector (Transmitter): codificación de señal (signal processing) y el modulador (carrier circuit).
- El medio de transmisión (channel).
- En la etiqueta (Receiver): el demodulador (carrier circuit) y el decodificador de canal (signal processing).

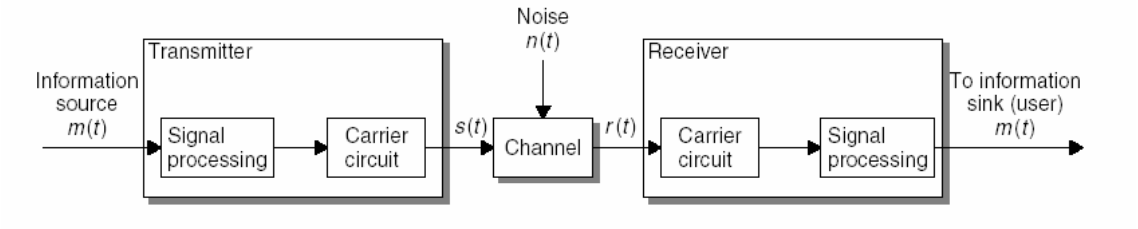


Figura 4.24 Bloques de funcionamiento de un sistema RFID.

Un sistema codificador de señal toma el mensaje a transmitir y su representación en forma de señal y la adecua óptimamente a las características del canal de transmisión.

Este proceso implica proveer al mensaje con un grado de protección contra interferencias o colisiones y contra modificaciones intencionadas de ciertas características de la señal.

4.7.1 Codificación en Banda Base

Los signos binarios “1” y “0” pueden ser representados por varios códigos lineales. Los sistemas de RFID suelen usar una de las siguientes codificaciones: NRZ, Manchester, Unipolar RZ, DBP (“diferential bi-phase”), Miller o Codificación Pulso-Pausa (PPC).

4.7.2 Código NRZ (No Return to Zero)

Un ‘1’ binario es representado por una señal ‘alta’ y un ‘0’ binario es representado por una señal ‘baja’. La codificación NRZ se usa, al menos, exclusivamente con una modulación FSK o PSK.

4.7.3 Código Manchester

Un ‘1’ binario es representado por una transición negativa en la mitad del periodo de bit y un ‘0’ binario es representado por una transición positiva. El código Manchester es, por lo tanto, también conocido como codificación de ‘parte-fase’ (splitphase coding).El código Manchester es frecuentemente usado para la transmisión de datos desde el transponder al lector basados en una modulación con sub-portadora.

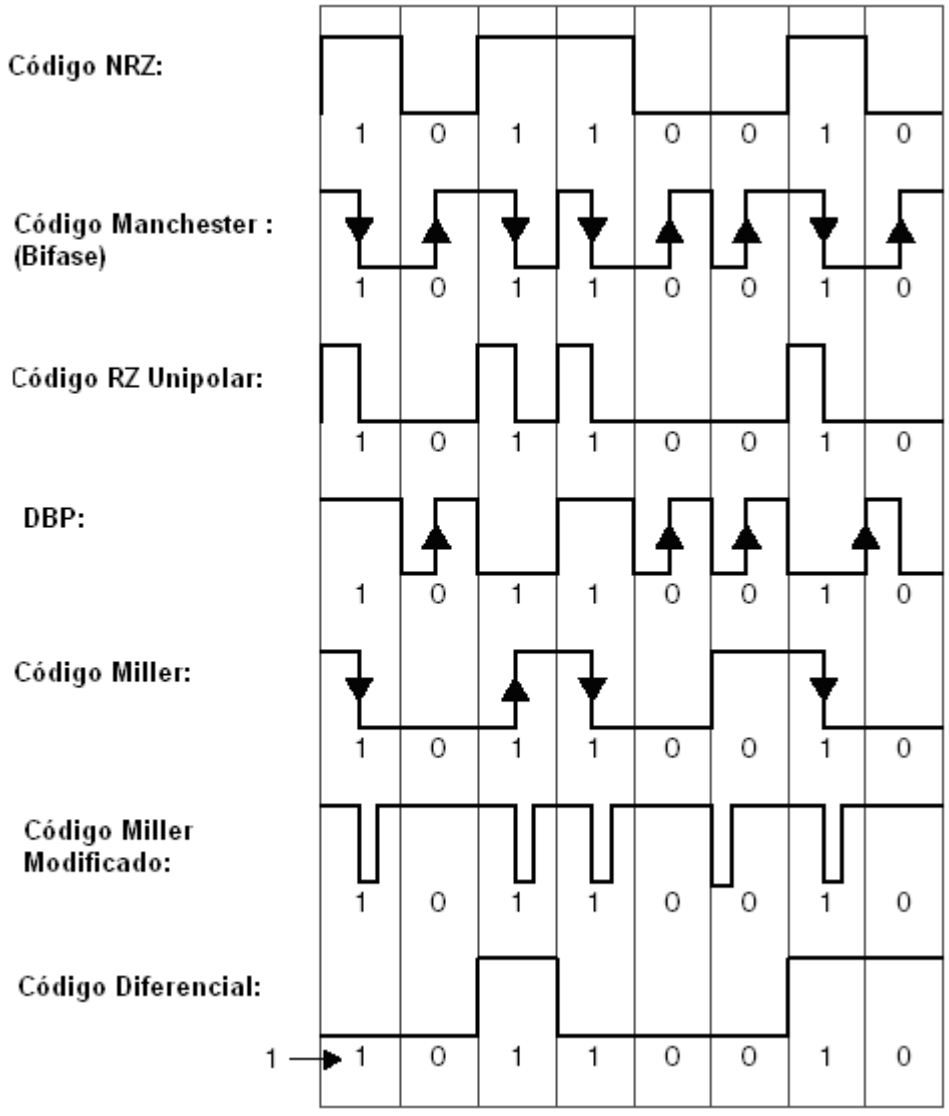


Figura 4.25 Representación gráfica de las principales codificaciones.

4.7.4 Código Unipolar RZ

Un ‘1’ binario es representado por una señal ‘alta’ durante la primera mitad del periodo de bit, mientras que un ‘0’ binario es representado por una señal ‘baja’ que dura todo el periodo de bit.

4.7.5 Código DBP

Un ‘0’ binario es codificado por una transición, de cualquier tipo, en mitad del periodo de bit. Un ‘1’ es codificado con una ausencia de transición. Además, el nivel de señal es invertido a inicio de cada periodo de bit, de modo que el pulso pueda ser más sencillamente reconstruido en el receptor si es necesario.

4.7.6 Código Miller

Un ‘1’ es representado por una transición de cualquier tipo en la mitad del periodo de bit, mientras que el ‘0’ binario es representado con la continuidad del nivel de la señal hasta el próximo periodo de bit. Una secuencia de ceros crea una transición al principio de cada periodo de bit, de modo que el pulso pueda ser más sencillamente reconstruido en el receptor si es necesario.

4.7.6.1 Código Miller Modificado

En esta variante del código Miller, cada transición es reemplazada por un pulso ‘negativo’. El código Miller Modificado es altamente recomendable para transmitir del lector al tag en sistemas RFID que usan acoplamiento inductivo.

Debido a la tan corta duración del pulso (tpulso << Tbit) es posible asegurar una continua alimentación del transponder debido al campo magnético del lector mientras dura la transferencia de información.

4.7.7 Codificación Diferencial

En la codificación diferencial cada ‘1’ binario que se tiene que transmitir causa un cambio en el nivel de la señal, así como para un ‘0’ el nivel permanece invariante. El código diferencial puede ser generado muy simplemente a partir de una señal NRZ usando una puerta XOR y un biestable D. En la siguiente figura vemos el circuito que logra este cambio en la señal.

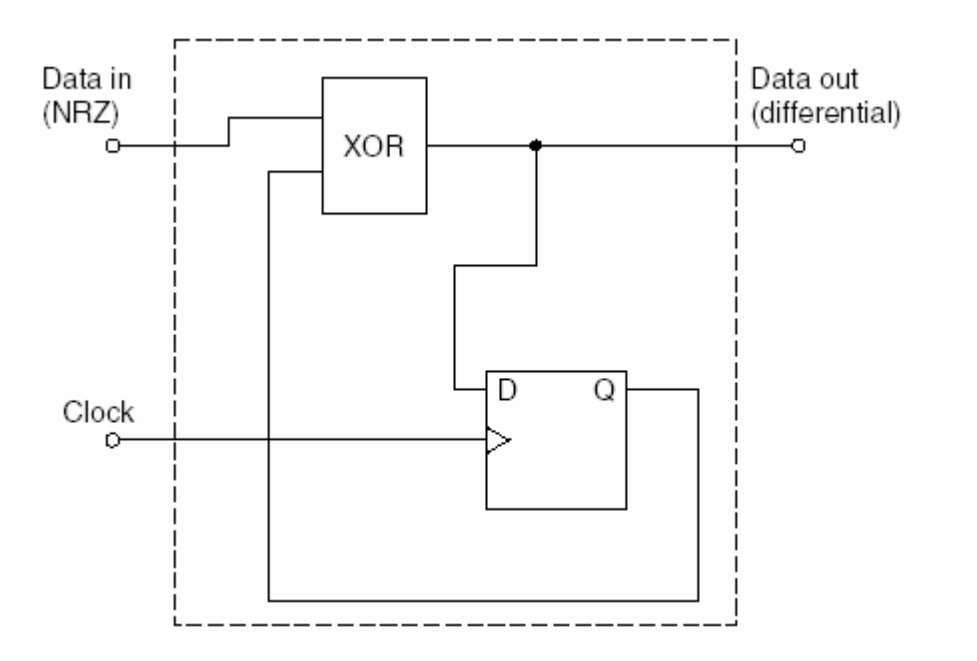


Figura 4.26 Generamos un código Diferencial a partir de uno NRZ.

4.7.8 Codificación Pulso-Pausa

En la codificación Pulso-Pausa (PPC – Pulse Pause Coding) un '1' binario es representado por una pausa de duración *t* antes del próximo pulso; un '0' binario es representado por una pausa de duración 2*t* antes del próximo pulso. Este método de codificación es popular para la transmisión de datos del lector a la etiqueta en los sistemas de RFID que usan acoplamiento inductivo.
Debido a la tan corta duración del pulso (tpulso << Tbit) es posible asegurar una continua alimentación del transponder debido al campo magnético del lector mientras dura la transferencia de información [20]

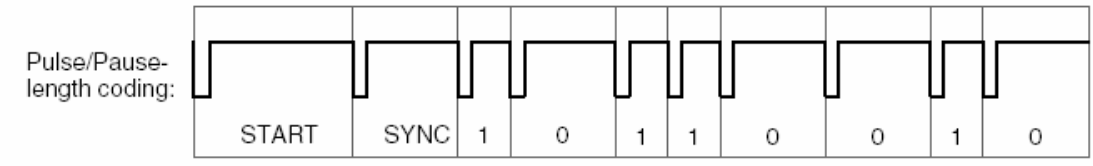


Figura 4.27 Posible transmisión de una señal usando PPC.

Debe tenerse en cuenta varias importantes consideraciones cuando se selecciona un posible sistema de codificación para un sistema RFID.

La consideración más importante es el espectro de la señal después de la modulación y lo susceptible que pueda ser a los posibles errores. Además, en el caso de tags pasivos (la alimentación de las etiquetas viene dada por el campo magnético que genera el lector), la fuente

de alimentación (es decir, la señal que emite el lector) no debe ser interrumpida por una combinación inapropiada los métodos de codificación de señal y modulación.

4.8 Modulaciones digitales usadas

La tecnología clásica de radiofrecuencia está fuertemente implicada con los métodos analógicos de modulación. Podemos diferenciar entre modulación de amplitud (AM), modulación de frecuencia (FM) y modulación de fase (PM), siendo éstas las tres principales variables de una onda electromagnética. Todos los demás métodos de modulación son derivados de cualquiera de uno de estos tres tipos.

Las modulaciones usadas en RFID son ASK (amplitude shift keying), FSK (frequency shift keying) y PSK (phase shift keying) [21].

4.8.1 ASK (Amplitude Shift Keying - Modulación por desplazamiento de amplitud

En Amplitude shift keying la amplitud de la oscilación de una portadora es variada entre dos estados *u0* y *u1* (keying) por un código de señal binario. *U1* puede tomar dos valores entre *u0* y 0. El intervalo entre *u0* y *u1* es conocido como el factor de trabajo (duty factor) *m*.

Es una modulación de amplitud donde la señal moduladora (datos) es digital.
Los dos valores binarios se representan con dos amplitudes diferentes y es usual que una de las dos amplitudes sea cero; es decir, uno de los dígitos binarios se representa mediante la presencia de la portadora a una amplitud constante, y el otro dígito se representa mediante la ausencia de la señal portadora. En este caso la señal moduladora vale

$$V\,m(t) = \begin{cases} 1 \text{ para un 1 binario} \\ 0 \text{ para un 0 binario} \end{cases}$$

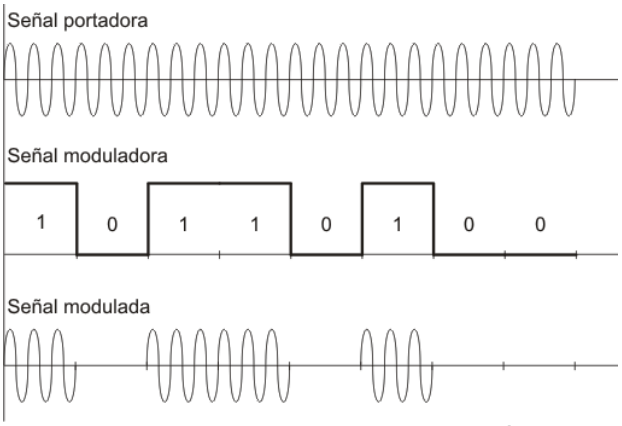


Figura 4.28 Diagrama del proceso de modulación por ASK

Mientras que el valor de la señal de transmisión (señal portadora) es dado por

$VP(t) = V\,psen(2fct)$

Donde Vp es el valor pico de la señal y fc es la frecuencia de la señal.

Como es una modulación de amplitud, la señal modulada tiene la siguiente expresión

$V(t) = V\,pvm(t)sen(2¼fpt)$

Mientras que el valor de la señal de transmisión (señal portadora) es dado por

$VP(t) = V\,psen(2¼fct)$

Donde Vp es el valor pico de la señal y fc es la frecuencia de la señal.

Como es una modulación de amplitud, la señal modulada tiene la siguiente expresión

$V(t) = V\,pvm(t)sen(2¼fpt$

$V\,(t) = (V\,psen\,(2¼fpt)$ para un 1 binario
0 para un 0 binario

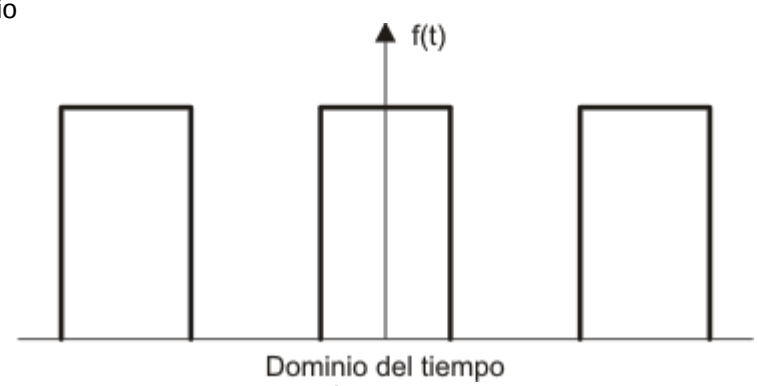


Figura. 4.29 Modulación ASK en el dominio del tiempo

Debido a que la señal moduladora es una secuencia periódica de pulsos, su espectro de frecuencias obtenido por medio del desarrollo en serie compleja de Fourier tiene la característica de la función *sampling*, véase figura (4.29) para el dominio del tiempo y la figura (4.30) para el dominio de la frecuencia.

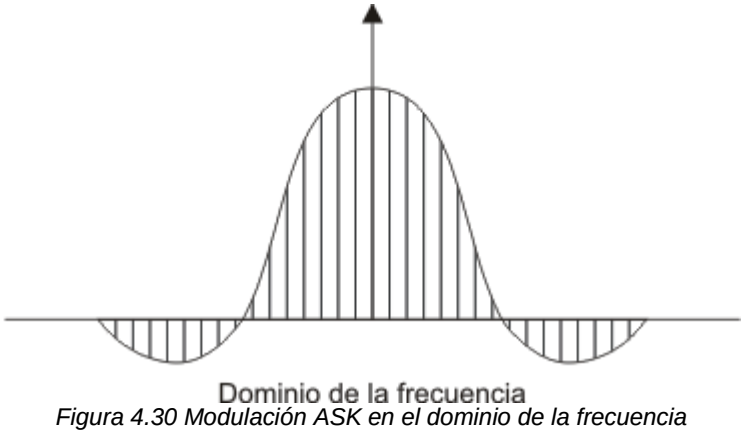


Figura 4.30 Modulación ASK en el dominio de la frecuencia

Este caso es similar a la modulación de amplitud para señales analógicas es decir, produce un desplazamiento de frecuencias, trasladando todo el espectro de frecuencias representativo de la secuencia de pulsos periódicos.

4.8.2 FSK (Frequency Shift Keying - Modulación por desplazamiento de frecuencia*)*

En esta modulación se usan dos ondas senoidales para representar *0 y 1*. Con FSK binario, existe un cambio en la frecuencia de salida cada vez que la condicion lógica de la señal de entrada binaria cambia. Por ejemplo, un *0* binario, tiene una frecuencia de 1.070 KHz (f1) y un *1* binario tiene una frecuencia de 1.270 KHz (f2), estas dos frecuencias se transmiten con alternancia para crear los datos binarios seriales.

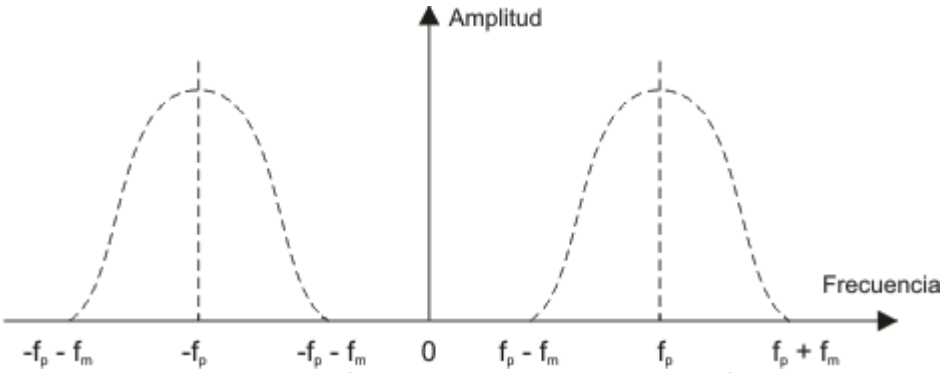


Fig. 4.31 Distribución de Frecuencias para la Modulación ASK

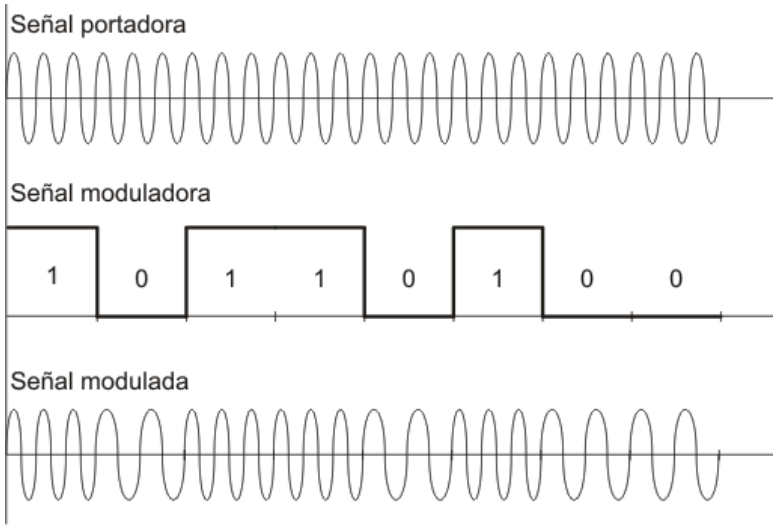


Figura. 4.32 Modulación con FSK

4.8.3 PSK (Phase Shift Keying - Modulación por desplazamiento de fase)

En esta modulación se usan dos ondas senoidales para representar *0 y 1*. Con FSK binario, existe un cambio en la frecuencia de salida cada vez que la condicion lógica de la señal de entrada binaria cambia. Un transmisor FSK binario sencillo se muestra en la ¯figura (4.32). Por ejemplo, un *0* binario, tiene una frecuencia de 1.070 KHz (f1) y un *1* binario tiene una frecuencia de 1.270

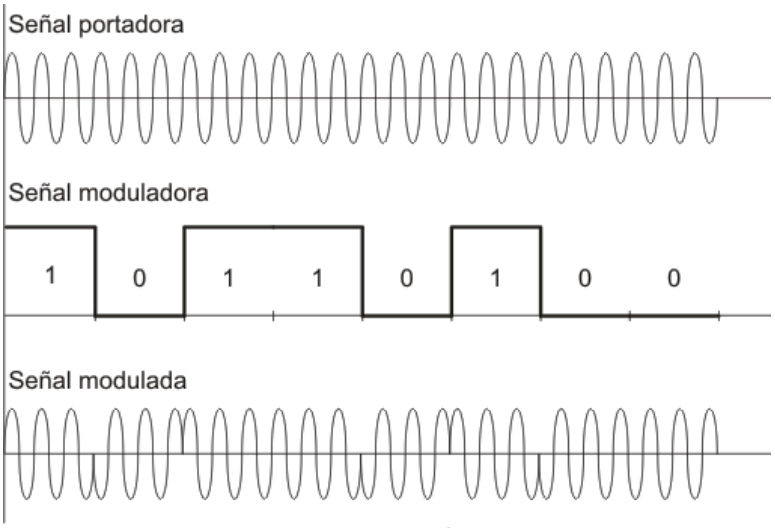


Figura 4.33 Modulación por PSK

4.8.4 Modulaciones que usan subportadora

En los sistemas de RFID, las modulaciones que usan subportadora son básicamente usadas cuando se trabaja con acoplamiento inductivo, normalmente en las frecuencias 6.78MHz, 13.56MHz o 27.125MHz en transferencias de información desde la etiqueta al lector.

Para modular la subportadora se puede elegir entre ASK, FSK o PSK. Una vez tenemos esta primera señal modulada (subportadora modulada), entonces se procede a una segunda modulación de la subportadora con la señal portadora (la que nos dará la frecuencia final a la que transmitiremos nuestra señal) [22].

El resultado de este proceso es una señal modulada con subportadora que transporta la información a una frecuencia 'menor', aunque la señal que lleva a la señal que contiene la información sí que va a una frecuencia mayor.

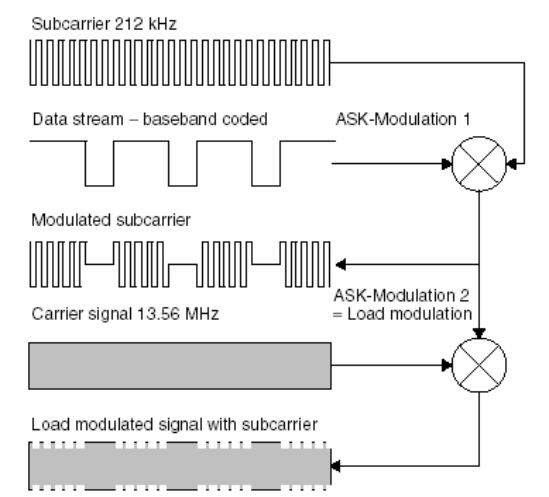


Figura 4.34 Proceso detallado de una modulación múltiple, con una subportadora modulada en ASK

La auténtica ventaja de usar una modulación con subportadora sólo se aclara cuando consideramos el espectro de la señal generada. Esta modulación inicialmente genera dos líneas espectrales a una distancia de ± la frecuencia de la subportadora *Fh* alrededor de la frecuencia central. La información se transmite, así, en las bandas laterales de las dos líneas subportadoras, dependiendo de la modulación de la subportadora generada a partir del código en banda base. Si la modulación usada es en banda base, las bandas laterales caerán justamente al lado de la señal portadora en la frecuencia central.

En las etiquetas que usan acoplamiento y que tienen unas pérdidas muy elevadas, la diferencia entre la señal portadora del lector *fT* y las bandas laterales recibidas de la modulación varían en un rango de entre 80 y 90 dB.

Una de los dos productos de la modulación con subportadora puede ser filtrado y remodulado usando la frecuencia de la modulación de las bandas laterales del flujo de datos. Aquí es irrelevante si se usa la banda 'alta' *fT* + *fH* o si se usa la banda 'baja' *fT* - *fH* ya que la información está contenida en ambas. La auténtica ventaja de usar una modulación con subportadora sólo se aclara cuando consideramos el espectro de la señal generada. Esta modulación inicialmente genera dos líneas espectrales a una distancia de ± la frecuencia de la subportadora *fH* alrededor de la frecuencia central. La información se transmite, así, en las bandas laterales de las dos líneas subportadoras, dependiendo de la modulación de la subportadora generada a partir del código en banda base. Si la modulación usada es en banda base, las bandas laterales caerán justamente al lado de la señal portadora en la frecuencia central.

En las etiquetas que usan acoplamiento y que tienen unas pérdidas muy elevadas, la diferencia entre la señal portadora del lector *fT* y las bandas laterales recibidas de la modulación varían en un rango de entre 80 y 90 dB.

Una de los dos productos de la modulación con subportadora puede ser filtrado y remodulado usando la frecuencia de la modulación de las bandas laterales del flujo de datos. Aquí es irrelevante si se usa la banda 'alta' *fT + fH* o si se usa la banda 'baja' *fT - fH* ya que la información está contenida en ambas.

4.9 Acoplamiento Inductivo

Este método se basa en el acoplamiento magnético entre el interrogador y el transpondedor, funcionamiento similar al de un transformador. La antena del lector genera un campo magnético que induce una corriente en la antena de la etiqueta, formada normalmente por una bobina y un condensador. La corriente inducida en el elemento acoplado (bobina) carga el condensador y éste proporciona el voltaje necesario para la transmisión.
Los sistemas que utilizan este principio de funcionamiento deben trabajar siempre en el campo cercano, que suele ser una distancia aproximadamente equivalente al diámetro de la antena. Para distancias superiores la fuerza del campo de la señal transmitida decrece con el inverso del cubo de la distancia o incluso con el inverso de la distancia elevada a su cuarta potencia (1/d3 o 1/d4), dependiendo de la orientación de la etiqueta respecto a la antena del lector, lo que dificulta en extremo una correcta recepción de la señal. Este fuerte debilitamiento de la señal puede ser positivo para aquellas aplicaciones donde se desee acotar la zona de cobertura del lector.

Normalmente este modo de funcionamiento se da en sistemas que trabajan a bajas frecuencias (BF y AF). Como el área de cobertura es pequeña, suele utilizarse con etiquetas pasivas, ya que éstas carecen de baterías de alimentación.

Por otro lado, cabe resaltar que la sensibilidad a las interferencias electromagnéticas es mayor en este tipo de sistemas, mientras que su coeficiente de penetración en materiales no conductivos es bueno.
Algunas de las aplicaciones que más utilizan los sistemas RFID inductivos son: las etiquetas inductivas de 1 bit para vigilancia electrónica de artículos (EAS), los controles de acceso y seguridad, sistemas antirrobo, identificación de animales e identificación de vehículos

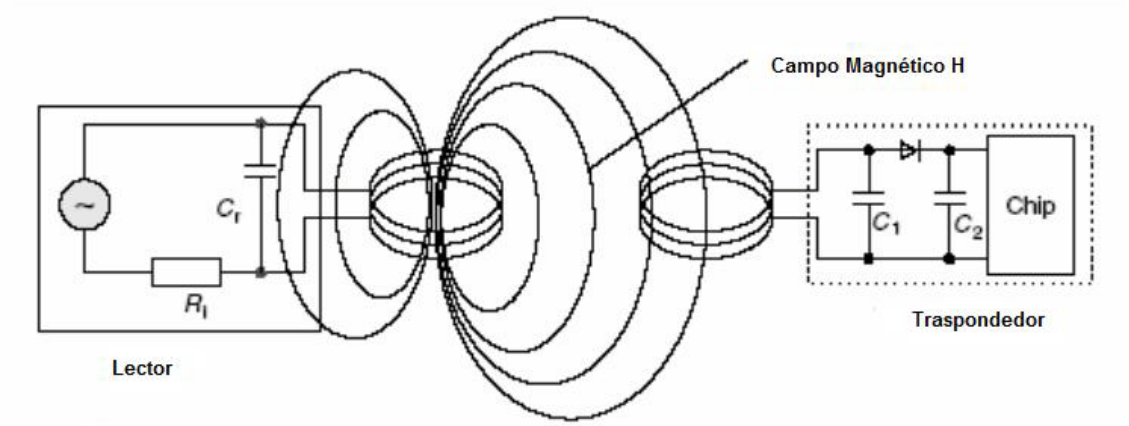


Figura 4.35 Esquema del acoplamiento inductivo entre lector y transponder.

En la Figura 4.35 podemos observar un esquema del acoplamiento inductivo. En estas frecuencias el campo creado por la antena del interrogador es la energía que aprovecha el transponder para su comunicación. Este campo está cerca de la antena del interrogador, lo que permite alcanzar unas distancias cercanas al diámetro de la antena. A distancias mayores la potencia necesaria es muy elevada. La bobina del lector genera un fuerte campo electromagnético, que penetra en la sección de la antena del transponder y en su zona cercana.

Las antenas de estos sistemas son bobinas, tanto del lector como del transponder, de gran tamaño, debido a la circunstancia de que la longitud de onda (λ) (como inverso de la frecuencia) es elevada. Estamos hablando de 2400m para frecuencias menores de 135KHz, y de 22,4m a una frecuencia de 13,56 MHz. Como esta longitud de onda es sensiblemente mayor que la distancia entre el lector y el transponder, el campo electromagnético puede ser tratado como un simple campo magnético alternante con respecto a la distancia entre transponer e interrogador [23].

Una parte pequeña del campo emitido penetra en la bobina del transponder. Se genera una tensión en la antena (bobina) por inducción. Este voltaje es rectificado y sirve como alimentación para el microchip del transponder encargado de almacenar la información. Como podemos observar en la Figura 2.8, un condensador es conectado en paralelo con la antena del lector, el valor de este condensador es seleccionado según la inductancia de la antena que forma un circuito paralelo de resonancia con una frecuencia de resonancia que tiene que coincidir con la frecuencia de transmisión del lector. En la antena del lector se generan grandes corrientes debido a la resonancia del circuito paralelo, lo que permite crear campos intensos necesarios para la comunicación entre lector y transponder.

La antena (bobina) del transponder y el capacitador en paralelo forman el circuito resonante a la misma frecuencia que emite el lector. El voltaje generado en el transponder es máximo debido a la resonancia producida por el circuito del transponder.

La eficiencia de la energía transmitida entre las antenas del lector y del transponder es proporcional a la frecuencia de operación, la relación entre el número de espiras que tienen las bobinas (en los transformadores conocido por el factor n), el área encapsulada por la antena del

transponder, el ángulo que forman las bobinas una en relación a la otra y la distancia entre las dos bobinas. Cuando la frecuencia se incrementa, la inductancia requerida en el transponder y el número de espiras decrece.
Como ejemplo, podemos decir que a una frecuencia de 135 KHz, el valor del factor n oscila entre 100 y 1000, y para una frecuencia de 13,56 MHz el valor del factor n=3-10.
Esto es debido a que el voltaje inducido en el transponder es todavía proporcional a la frecuencia de resonancia, en cambio el número de espiras de la bobina apenas afecta a la eficiencia de la energía transmitida a altas frecuencias.

Transferencia de datos entre transponder y lector

En este apartado para trabajar con sistemas de acoplamiento inductivo se suelen usar tres tipos:

- Load modulation
- Load modulation con subportadora
- Subarmónicos

Load modulation – Modulación de Carga

Se fundamenta en el funcionamiento de un transformador, siendo la bobina primaria la del lector y la secundaria la del transponder. Esto es cierto si la distancia entre las bobinas no es mayor de 0,16λ, por lo que el transponder y el lector deben estar próximos. Si un transponder en resonancia se encuentra dentro del campo magnético de un lector, coge energía de ese campo magnético.

El resultado del “feedback” del transponder en la antena del lector puede ser representado como una impedancia (T *Z)*. Conectando y desconectando la resistencia de carga presente en la antena del transponder se consigue variar el valor de *T Z,* con lo que el voltaje que existe en la antena del lector también varía. Esto tiene un efecto en la modulación de amplitud del voltaje del lector por culpa del transponder remoto. El tiempo en el que se desconecta y se conecta la resistencia de carga es controlado por los datos, es lo que se usa para enviar los datos del transponder al lector.

Load modulation con subportadora

Debido al acoplamiento débil que se realiza entre lector y transponder, las fluctuaciones que se producen en la tensión en la antena del lector (la información) en varios órdenes de magnitud inferior a la tensión de salida del propio lector. En la práctica para un sistema de 13,56 MHz, se entrega a la antena un voltaje de 100V en resonancia, la señal recibida del transponder es del orden de 10mV.

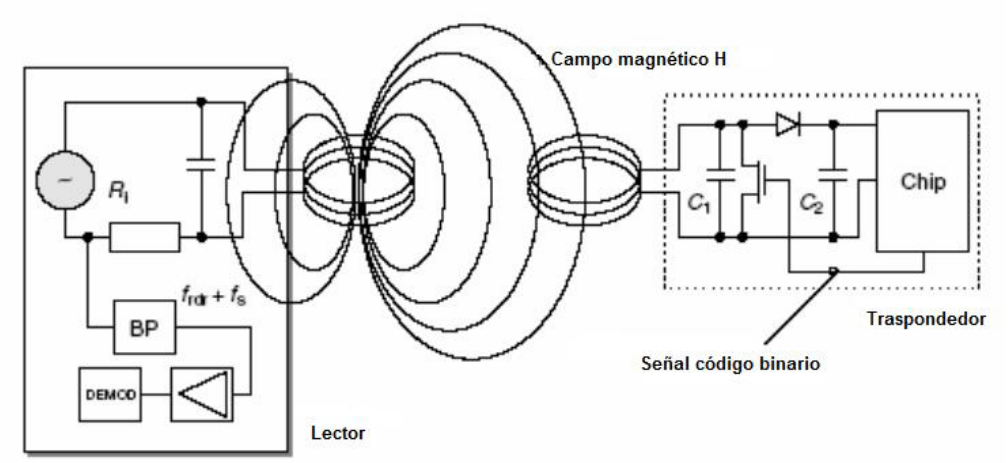


Figura 4.36 Generación de load modulation conectando y desconectando la resistencia del drain-source del FET del chip. El lector tiene un circuito capaz de detectar la subportadora.

Detectar esta fluctuación requiere una circuitería complicada, como solución se usan las bandas contiguas a la modulación creada. Para ello se incorpora una nueva resistencia de carga en el transponder que se conecta y desconecta a una frecuencia elevada fs, entonces dos líneas espectrales son creadas a una distancia fs de la frecuencia de resonancia entre lector y transponder. Uno de los métodos posibles es utilizar un transistor FET en el transponder, como vemos en la Figura 4.37.

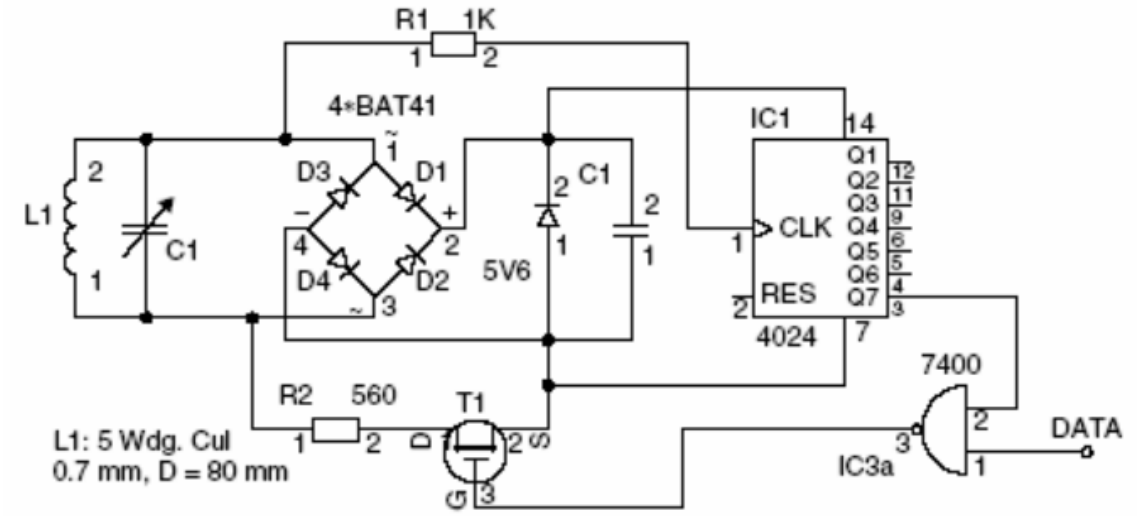


Figura 4.37 Ejemplo más detallado de un generador de modulación de carga con subportadora en sistema de acoplamiento inductivo.

En esas frecuencias conocidas como subportadoras, es más fácil detectar las variaciones de tensión. La información se puede modular en ASK, FSK o PSK con el flujo de datos. Esto significa una modulación de amplitud en la subportadora. Por último solo se requiere un filtro de paso banda para aislar una de las dos subportadoras.

Debido a la amplia banda de guarda que requieren estos filtros, este procedimiento sólo es usado en la banda ISM en las frecuencias 6,78 MHz, 13,56 MHz y 27,125 MHz.

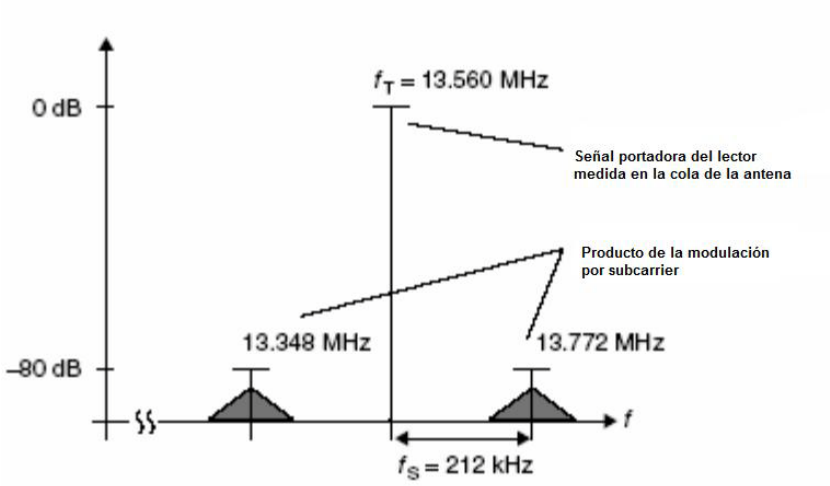


Figura 4.38 La load modulation crea dos subportadoras a una frecuencia fs de la frecuencia de transmisión del lector. La información se encuentra en las bandas laterales de las dos subportadoras.

Sub armónicos

Basado como su propio nombre indica en la utilización de subarmónicos de una frecuencia fA, es decir, f1=fA /2, f2=fA /3, etc. Se suele utilizar el primer subarmónico, es decir la mitad de la frecuencia en la que transmite el lector. La señal después del divisor es modulada por el flujo de datos y enviada para el transponder. Esta será la frecuencia a la que responda el transponder. El transponder necesitará un divisor binario de frecuencia para realizar dicha operación. La frecuencia de operación más popular para los sistemas subarmónicos es de 128 kHz. Por lo que la frecuencia de respuesta del transponder es de 64 kHz.

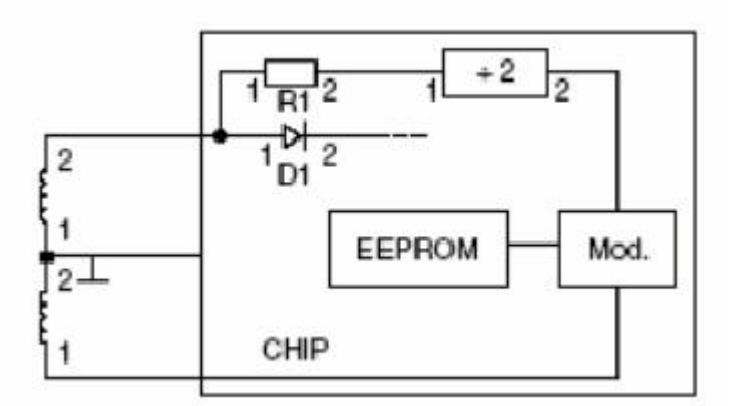


Figura 4.39 Diseño de un transponder que usa subarmónicos,

4.10 Acoplamiento Backscatter

Otro sistema de transferencia de información son los sistemas “long-range”, que como su propio nombre indica son de largo alcance, mayores a 1 m. Estos sistemas se basan en el uso de ondas electromagnéticas en el rango de UHF o microondas. La mayoría de estos sistemas son conocidos como sistemas “backscatters” debido a su principio de operación. Existen otros sistemas de largo alcance que utilizan ondas acústicas de superficie en el rango de microondas.

Todos estos sistemas “long-range” operan en los rangos de UHF, 868 MHz (Europa) y 915 MHz (USA) y en rango de microondas en 2,5 GHz y 5,8 GHz. La principal ventaja de trabajar a estas frecuencias es tener una longitud de onda corta, lo que permite la construcción de antenas de un tamaño muy pequeño y de gran eficiencia.

Los sistemas que usan el principio backscatter tienen unos alcances típicos de 3 m en transponders pasivos (sin baterías) y de unos 15 m en transponders activos. La batería de los transponders activos no proporcionan la energía necesaria para la comunicación entre lector y transponder, únicamente alimentan el microchip en su proceso de almacenamiento y consulta de memoria. La energía para la transmisión entre el transponder y el lector, por tanto, es únicamente la extraída del campo electromagnético generado por el interrogador al realizar la comunicación con el transponder [23]

Básicamente el transponder modula la información recibida desde el lector variando la impedancia de la antena, esto se realiza variando el valor de la resistencia de carga R_L. Podemos ver en la Figura 4.40 al igual que en el ejemplo de acoplamiento inductivo, la impedancia del transponder es modulada por el transistor FET del chip.

El lector tiene un acoplador direccional para separar la señal transmitida de la señal recibida mucho más débil. El interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal. La señal recibida por el interrogador desde la tarjeta está a un nivel de unos -60db por debajo de la portadora de transmisión del propio sensor.

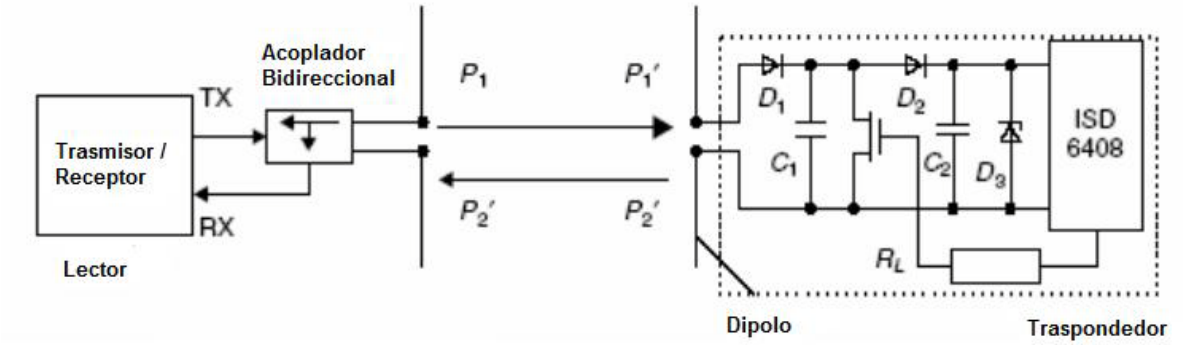


Figura 4.40 Esquema del funcionamiento de los sistemas backscatter.

En referencia a la energía necesaria para la transmisión de información a estas frecuencias, se debe realizar con anterioridad un cálculo de las pérdidas por espacio libre en relación a la distancia

r entre transponder y lector, podemos ver la ecuación (4.32). En este caso tendremos como variables las ganancias de las dos antenas y la frecuencia a la que opera el sistema. Por lo que respecta a las unidades, la frecuencia está expresada en Hz y la distancia en m.

$$a_F = -147.6 + 20\log(r) + 20\log(f) - 10\log(G_T) - 10\log(G_R) \quad (4.32)$$

Las pérdidas en espacio libre son la relación entre la potencia emitida por el lector y la potencia recibida en el transponder, todo esto a una determinada frecuencia.

Usando la tecnología de semiconductores de baja corriente los chips de los transponders pueden operar con un consumo no mayor de 5μW. Existen sistemas que incorporan al transponder unas baterías adicionales, lo que implicaría un aumento en el rango de alcance, estos sistemas permiten incluso optimizar el consumo de estas baterías, cuando el transponder no está en el rango de alcance del lector, las baterías permanecen en un estado de desconexión hasta que nuevamente se encuentran bajo la acción del interrogador. En este estado de "stand-by" el consumo es de pocos μA. El chip no es reactivado hasta que recibe una señal lo suficientemente fuerte en el rango de alcance del lector para volver al estado normal.

En la Tabla 4.2 podemos observar las perdidas en espacio libre a diferencias frecuencias, vemos como se esperaba que a más frecuencia y más distancia, más pérdidas.

Distancia r	868 MHz	915 MHz	2.45 MHz
0.3 m	18.6 dB	19.0 dB	27.6 dB
1 m	29.0 dB	29.5 dB	38.0 dB
3 m	38.6 dB	39.0 dB	47.6 dB
10 m	49.0 dB	49.5 dB	58.0 dB

Tabla 4.2 Perdidas en espacio libre considerando la ganancia del transponder como 1.64 (dipolo), y la ganancia de la antena del lector como 1 (emisor isotrópico)

La principal diferencia con los sistemas inductivos es de donde proviene la energía que aprovecha el transponder para realizar la comunicación, mientras los sistemas a una frecuencia más elevada utilizan las ondas electromagnéticas, consiguiendo así un rango de alcance mayor, los sistemas inductivos utilizan la energía que una antena crea a su alrededor.

Transferencia de datos entre transmisor y transponder

Por la tecnología de radares sabemos que las ondas electromagnéticas se reflejan en objetos con dimensiones mayores a la mitad de la longitud de onda. La eficiencia con la que estos objetos reflejan las ondas se describe por el término conocido como "reflection cross-section". Una pequeña parte de la potencia emitida por la antena del lector es absorbida por la antena del transponder, pasa por la antena del transponder como un voltaje de HF y después es rectificado por diodos. El voltaje debe ser suficiente para servir como alimentación para rangos pequeños. Una proporción de la potencia absorbida es reflejada por la antena y retornada [24].

Las características de esta reflexión pueden ser influenciadas por las alteraciones en la carga de la antena. Para transmitir del transponder al lector, la resistencia de carga presente en el transponder conectada e paralelo con la antena, se conecta y desconecta según el flujo de datos. La amplitud de esa onda reflejada desde el transponder es lo que se modula, de ahí el nombre de modulación backscatter. Esta potencia reflejada es radiada en el espacio libre, una pequeña parte de esa potencia es recogida por la antena del lector. Esa potencia, el lector la recoge por medio de un acoplador direccional, despreciando así la potencia que emite él mismo la cual es sustancialmente mayor.

4.11 Acoplamiento Close Coupling

Los sistemas de acercamiento cercano están diseñados para rangos de alcance entre 0.1 cm y un máximo de 1 cm. El transponder cuando se realiza la comunicación suele estar en el centro de un aro que es la bobina del lector, o bien, en el centro de una bobina en forma de "u". El funcionamiento de las bobinas del transponder y del lector es el mismo que el de un transformador. El lector representa las espiras primarias y el transponder las secundarias del transformador. Podemos verlo en la Figura 4.41.

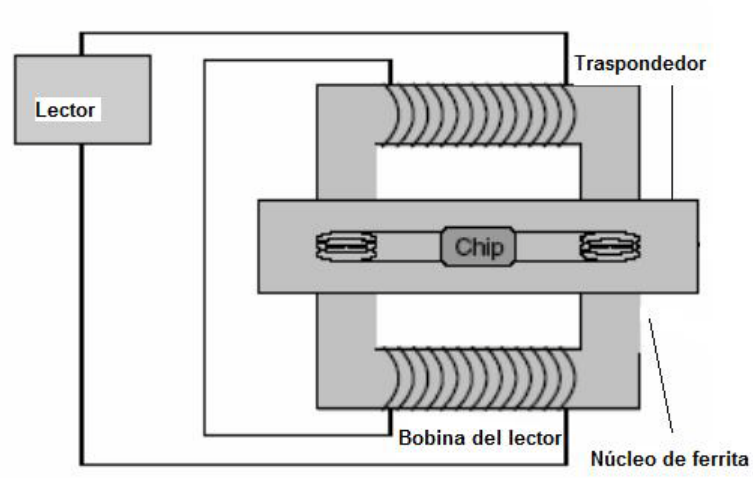


Figura 4.41 En los sistemas Close Coupling el transponder debe insertarse en el reader para producirse el acoplamiento magnético entre bobinas.

Una corriente alterna de alta frecuencia en las espiras primarias genera un campo magnético de alta frecuencia que se transmite por la bobina del transponder. Esta energía es rectificada y proporciona la alimentación al chip del transponder. Debido a que la tensión inducida es proporcional a la frecuencia de la corriente entrante, la frecuencia seleccionada debe ser lo más elevada posible [25]. En la práctica son usados rangos entre 1 – 10 MHz. Para mantener las perdidas en el núcleo del "transformador" estas bobinas son elaboradas con ferrita, un material que optimiza las perdidas a estas frecuencias.

A diferencia con los sistemas de acoplamiento inductivo y microwave, la eficiencia de la energía transmitida del lector al transponder es excelente, por eso suelen ser usados en sistemas que necesitan del uso de chips potentes, que consuman mucha energía, como por ejemplo microprocesadores.

5. Aplicaciones

La principal característica de la tecnología RFID es la capacidad de identificar, localizar, seguir o monitorizar personas u objetos sin necesidad de que exista una línea de visión directa entre la etiqueta y el lector (al menos en algunas de las frecuencias de trabajo, como hemos visto en una sección anterior). Alrededor de esta funcionalidad han surgido una gran variedad de aplicaciones perfectamente adaptables a una gran diversidad de sectores industriales y de servicios lo que ha permitido en la última década el crecimiento en el desarrollo de la industria de la RFID principalmente en Europa y Estados Unidos.

Es en este capítulo que se hace un análisis significativo de las ramas más importantes de la industria y de los servicios que han adaptado la tecnología RFID para facilitar la fabricación, empaque, monitoreo, seguridad, gestión de personal e infinidad de procesos y procedimientos para beneficio de las empresas.

5.1 Principales áreas de aplicación

En el ámbito de las aplicaciones de negocios, comerciales y de servicios, el potencial de negocio de las aplicaciones RFID es muy grande, como muestran los siguientes ámbitos:

- Transporte y distribución.
  - Seguimiento de activos.
  - Aeronaves, vehículos, ferrocarriles.
  - Contenedores.
  - Sistemas de localización en tiempo real.

- Empaquetado de artículos.
  - Gestión de la cadena de suministro.
  - Seguimiento de cajas y palés.
  - Seguimiento de elementos.
  - Industria farmacéutica.
  - Inventario y stocks.

- Industria y fabricación.
  - Estampación.
  - Flujo de trabajo.

- Seguridad y control de accesos.
  - Gestión de pasaportes y visados.
  - Seguimiento de niños.
  - Seguimiento de animales.
  - Seguimiento de equipajes.
  - Prevención de falsificaciones.
  - Acceso a ordenadores.
  - Identificación de empleados.
  - Acceso a aparcamientos.
  - Acceso a laboratorios, recintos, etc.
  - Peajes.
  - Pagos automáticos.
  - Reconocimiento de clientes.

- Monitorización y censado.
  - Presión, temperatura, volumen y peso.
  - Aplicaciones de localización.

- Sistemas de biblioteca.
  - Acceso y gestión de libros.
  - Acceso y gestión de todo tipo de objetos.

En concreto, sin ánimo de ser exhaustivos, podemos citar algunos de los usos actuales de RFID:

- Puntos de venta.
- Sistemas de identificación automática de vehículos.
- Control de acceso a edificios o recintos en el interior de edificios.
- Identificación de animales de granja y ganado.
- Seguimiento de activos.
- Identificación de mascotas.
- Logística y gestión en almacenes mayoristas (Ejemplo, Kimberly Clark).
- Seguimiento de productos en cadena de suministro (por ejemplo, seguimientos de palés, Walmart, DoD, Target, Tesco, Metro Group).
- Seguridad de productos.
- Seguimiento de materiales para movimiento en fábrica.
- Aplicaciones de trazabilidad.
- Sistemas de pago de peajes.
- Entrada y salida de libros en bibliotecas

- Seguimiento de equipajes en aeropuertos
- Arranque de automóviles (Toyota, Renault, Lexus y Audi).
- Deportes (aplicación en el seguimiento de deportistas en la Maratón).
- Entradas (por ejemplo, uso en la Master Cup de Tenis en 2005 o en la 2005 Canon Expo en París).
- Seguimiento de personas (en aplicaciones médicas o como medida de seguridad, por ejemplo, para identificación de recién nacidos en hospitales).
- Aplicaciones farmacéuticas.

Además de estas aplicaciones industriales mencionadas, existen otros ámbitos en los que los dispositivos RFID aparecen como una opción altamente prometedora. Uno de ellos es el de los sistemas de seguridad fronteriza. En este ámbito, la función de los sistemas de identificación biométrica con las capacidades de localización e identificación de los dispositivos RFID está teniendo resultados muy positivos. Pueden aplicarse a:

- Identificación de vehículos, conductores, pasajeros y personal en puestos fronterizos.
- Sistemas de registro de vehículos.
- Control de acceso de vehículos en recintos protegidos.
- Trazabilidad de bienes importados, y seguridad en las importaciones.
- Seguimiento e identificación de contenedores.
- Control de pasajeros, equipajes y carga en transportes aéreos.

Otro de los aspectos en los que la RFID puede resultar de utilidad es el de la mejora en la eficacia policial y judicial. Los aspectos donde la tecnología RFID puede contribuir son:

- *Mejora de la eficacia policial*. En este ámbito podemos destacar:
  - Gestión y seguridad en el almacenamiento de pruebas policiales.
  - Localización policial en comisarías.
- *Mejora de la seguridad policial*. En este ámbito podemos destacar:
  - Protección de armas de fuego.
  - Monitorización de patrullas.
- *Lucha contra el crimen*. En este ámbito podemos destacar:
  - Protección de bienes.
  - Placas de matrículas de automóviles.
  - Carnés y permisos de conducción

La Tabla 5.1 da una idea de los usos y volúmenes negocio de RFID en diversos países.

APLICACION	VOLUMEN POTENCIAL	COMENTARIOS
Identificación. Tarjetas inteligentes inalámbricas	Italia. 50 millones U.K. 58 millones India. 500 millones China. 970 millones	China envió 8 millones de tarjetas de este tipo a sus países vecinos. En 2010 China necesitará del orden de 1000 millones de tarjetas, y otros países tendrán necesidades similares
Pasaportes electrónicos	400 millones anuales	EEUU, UK, Tailandia y Australia, entre otros países, tienen en sus planes incluir chips RFID en los pasaportes. Ya existen las primeras versiones operativas.
Llantas de automóviles	200 millones anuales	El Acta TREAD en EEUU ordena utilizar RFID para monitorizar la presión y la temperatura de la llantas
Lavanderías	Hasta 1000 millones de etiquetas al año	Se trata de un área con grandes potencialidades e crecimiento. Ya se han vendido del orden de 70 millones de etiquetas.
Archivo	Hasta 100.000 millones de Etiquetas	Mercado potencialmente masivo, que incluye las bibliotecas y las entradas a todo tipo de eventos.
Transportes	2000 millones por año.	En palés y cartones de embalaje se pueden necesitar varios miles de millones de etiquetas al año, sin contar necesidades en otros elementos como Vds., CD, hojas de afeitar, etc. O marcado de equipajes en aeropuertos.

Tabla 5.1 Usos y volúmenes de negocio de RFID a nivel global

Si nos fijamos ahora en los casos de estudio almacenados en IDTechEx15 (empresa que recopila casos de estudio a nivel mundial, así como otra información relevante relacionada con la tecnología RFID), la Figura 5.1 muestra la distribución de los casos por ámbitos de aplicación.

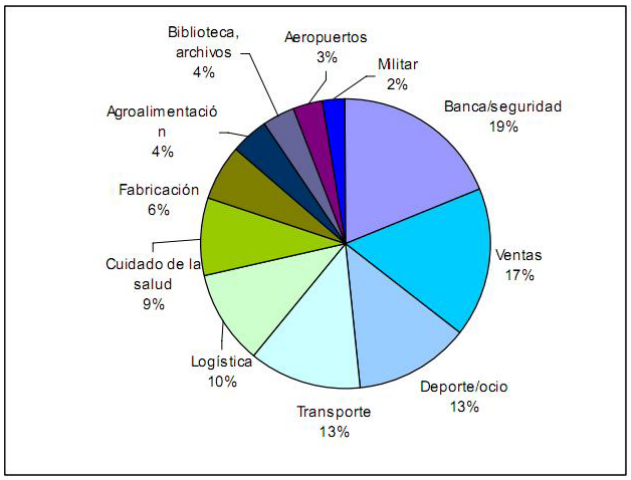


Figura 5.1 Distribución de los casos de estudio almacenados en IDTechEx (julio de 2007).

La tecnología RFID se ha ido haciendo un hueco en el mercado, con un progreso espectacular en los últimos años. Muchos son los sectores que se han visto beneficiados con la incursión de nuevos sistemas de identificación basados en la tecnología RFID, como los transportes, las tarjetas inteligentes, expedición de tickets, control de acceso, identificación de animales, identificación de contenedores, medicina o la industria del automóvil.

5.2 Control de accesos

Las aplicaciones en este campo han sido uno de los puntos fuertes de los sistemas RFID. No son unos sistemas nuevos, ya que llevan varios años usándose en empresas o recintos, para controlar el acceso a sus instalaciones. También se suelen usar para el acceso a estacionamientos. Estas tarjetas son cada vez más funcionales, pudiendo permitir no sólo el acceso a distintas zonas, sino también a máquinas expendedoras o para pagos pequeños, por ejemplo en una cafetería de la empresa.

5.3 Identificación de equipajes en el transporte aéreo

Es un claro ejemplo de una aplicación que puede reducir costos y tiempo a las compañías aéreas y a los aeropuertos. Se puede sustituir personal si el equipaje es direccionado mediante sensores, por toda la cadena, que detectan el transponder con la información del avión en el cual tiene que ser cargado. Aparte de esta ventaja, también es más cómodo a la hora de identificación del equipaje sobre posibles pérdidas. Además no supone un gasto excesivo para la rentabilidad que el sistema puede ofrecer. No ocurre ningún problema al ponerlo sobre las etiquetas ya usadas en los aeropuertos ni importa que los equipajes estén orientados de cualquier forma o apilados de cualquier manera.

Un sistema RFID es mucho más eficaz en esta aplicación que los usados códigos de barras. Las principales ventajas por las que las compañías del sector están incorporando estos sistemas son:

- La posibilidad de convivir con los sistemas de códigos de barras ya existentes y sus scanner. Así como encajar perfectamente en los sistemas de control de aeropuertos y sus sistemas de seguridad especialmente.
- Incorporar más información en el dispositivo sin aumentar el tamaño.
- La información va incorporada en la propia etiqueta, por lo que se ahorra la comunicación continua con una base de datos.

La mayoría de estos sistemas trabajan a una frecuencia de 13,56 MHz, como es el sistema instalado por los aeropuertos de Manchester y Munich en 1999, en acuerdo con la compañía aérea British Airways. Podemos ver un ejemplo de estas etiquetas en la Figura 5.2.

Figura 5.2 Etiqueta identificadora de RFID en el aeropuerto de Munich.

5.4 Industria del automóvil

A principios de los 90 aparecieron sistemas RFID con transponders de sólo lectura destinados a la inmovilización de automóviles como un adelanto importante en la seguridad de los vehículos ante posibles robos. Los transponders de estos sistemas eran muy pequeños (cabían en la llave), no necesitaban baterías y eran de solo lectura.

Cada uno de estos transponders disponía de un único y fijo código de seguridad. Su funcionamiento era sencillo, cuando el propietario giraba la llave producía unas señales electromagnéticas que eran las que verificaban la llave y permitían el arranque del motor.

En el sector de la seguridad en el automóvil, también se diseñó un sistema que inmovilizase el vehículo, de modo que cuando el usuario cerraba la puerta con su mando, generaba un código que

recibía el coche y que volvía a enviar al transponder del mando a modo de confirmación. Podemos ver el funcionamiento en Figura 5.3.

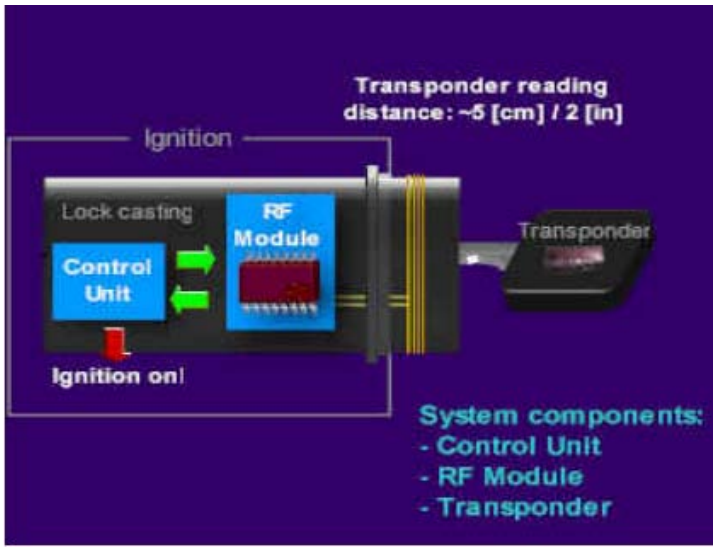


Figura 5.3 Esquema de funcionamiento del sistema de seguridad de automóvil.

Otra aplicación en los automóviles que cada vez incorporan más, es la tarjeta identificadora que permite que el vehículo se abra sin necesidad de introducir ninguna llave. Sólo necesita que el propietario se acerque lo suficiente al vehículo con su tarjeta para que detecte un transponder, lo confirme y proceda a desbloquear las puertas. Es un sistema más útil que el tradicional "mando a distancia"; en el que había que presionar un botón para abrir el vehículo.

5.5 Comercio a distancia

Los sistemas RFID son los suficientemente seguros como para permitir pagos con ellos. Por ejemplo pagar combustible o usarlo en una máquina expendedora de comida o bebida. El cliente paga con su teléfono móvil o con una llave especial.

Además proporciona información a las empresas sobre los gustos del cliente, pudiendo ofrecerle un servicio con más calidad.
El transponder posee una información única programada que al pasar cerca del lector es identificada, se verifica la autenticidad del transporte, y se pide permiso para la transacción.

Por lo que hace al sistema de pago en gasolineras, es muy cómodo tanto para el cliente como para la estación de servicio. Aumenta el número de coches que pueden repostar por hora, así como ofrece al usuario un tiempo menor de espera. Existen dos métodos:

- *Método Token:* Es muy similar al pago en dispensadores de bebida, cada transponder tienen un único código ya programado, que además está relacionado con una tarjeta de

crédito. Se inicia la comunicación con el lector situado en el surtidor, nunca se envía el número de la tarjeta de crédito que no está ni siquiera almacenado en el transponder. Se pide autorización a través de la estación de servicio, y se le permite repostar.

- *Método "Manos Libres":* Es un sistema que difiere del anterior en que el transponder va adherido al cristal trasero del coche. Se realizan las mismas operaciones que en el caso anterior pero con más velocidad; con lo que la comunicación se realiza incluso antes que el cliente baje del coche.

Están solo algunas de las aéreas de aplicación de la tecnología RFID, sin embargo existen muchas más en los diferentes sectores de la industria y de servicios como son: en el sector ganadero por ejemplo se utiliza para rastrear y monitorear ganado en grandes extensiones de tierra para su pronta localización y conteo, en el sector de la salud se ha utilizado en diferentes aéreas una de ellas es el rastreo de personas enfermas que padecen alguna enfermedad mental en hospitales psiquiátricos, en el sector de la seguridad ha venido teniendo buena aceptación en aéreas como son el monitoreo de reos de alta peligrosidad en prisiones y en la monitorización de personas que han sido pre liberadas o bajo libertad causal, en lo concerniente a la industria del automóvil más recientemente se ha desplazado a la tecnología GPS(Global Positioning System- Sistema de Posicionamento Global) en lo concerniente a la localización de vehículos ya que dicha tecnología no permite el rastreo de los vehículos dentro de contenedores metálicos de gran tamaño o inclusive debajo de puentes o grandes edificaciones, la tecnología RFID por lo contrario permite localizar los vehículos inclusive dentro de contenedores metálicos (dependiendo de la tag incrustada y el tipo de antenas usadas) y edificaciones debido al uso de la radiofrecuencia.

6. Seguridad y Privacidad

Los sistemas de RFID se están usando cada vez más en aplicaciones de alta seguridad como son los sistemas de acceso o para realizar pagos y tickets de caja. Por eso mismo el uso de los sistemas de identificación por radiofrecuencia necesita del uso de sistemas de seguridad para protegerlos de posibles ataques.

La seguridad es un aspecto especialmente importante. A menudo abrazamos las nuevas tecnologías sin preocuparnos excesivamente de la seguridad. Podemos pensar en los ordenadores (con la aparición de los virus), en Internet (con la aparición de diversos tipos de ataques a los ordenadores conectados a la red), etc. RFID es una tecnología de reciente aparición y usos muy prometedores, y si no se dota de la debida seguridad, aparecerán sin duda problemas a la hora de prestar servicio. De hecho, RFID se está empezando a utilizar en muchísimas aplicaciones sin demasiadas preocupaciones en los aspectos de seguridad.

Es en el presente capitulo donde se hace estudio de los aspectos de seguridad en los sistemas RFID, así mismo se hace un análisis de los principales algoritmos de seguridad y encriptación utilizados en los dispositivos RFID, todo esto con la finalidad de comprender la importancia de seguridad en la implementación de sistemas basados en esta tecnología.

6.1 Tipos de Ataques a sistemas RFID

A pesar de ser una tecnología joven, ya han aparecido casos de compromisos de seguridad en sistemas RFID. Por ejemplo, en enero de 2005 un grupo de estudiantes consiguió romper el cifrado del sistema de puntos de venta RFID de ExxonMobil.

Es posible monitorizar los niveles de potencia de etiquetas RFID utilizando una antena direccional y un osciloscopio. Los patrones que aparecen en los niveles de potencia pueden servir para determinar si la contraseña es aceptada o no por el dispositivo RFID. Utilizando esta información y un teléfono móvil podría comprometerse la información que se transmite vía RFID. Por abundar más en estas ideas, un grupo de la Free University de Holanda se ha dedicado a crear virus para RFID a modo de “prueba de concepto”. Consiguieron crear malware que se almacenaba en una etiqueta RFID, de donde podía pasar al lector y de allí
al sistema de explotación [27]

La forma más simple de ataque a un sistema RFID es evitar la comunicación entre el lector y la etiqueta. Esto se puede realizar de forma tan simple como apantallar con metales.

Existen otras formas de ataque más sofisticadas, cuyo blanco son las comunicaciones en radiofrecuencia. Las más importantes se pueden clasificar en cuatro tipos: *Spoofing,* Inserción, *Replay* y Denegación de servicio.

- *Spoofing*

Este tipo de ataque consiste en suministrar información falsa que parece ser válida y que es aceptada por el sistema. Por ejemplo, se podría enviar un código electrónico de producto (EPC) falso, cuando el sistema espera uno correcto.

- *Inserción*

Este tipo de ataque inserta comandos del sistema donde habitualmente se esperan datos. Por ejemplo, inserción de comandos SQL en una base de datos o inserción de comandos donde deberían ir, por ejemplo, códigos EPC.

- *Replay*

En este tipo de ataque, se intercepta una señal RFID y se graban los datos. Posteriormente se retransmiten al sistema, que los acepta como válidos.

- *Denegación de servicio (DOS)*

En este tipo de ataques, se colapsa al sistema alimentándole con más datos que los que puede manejar. Hay una variante conocida como RF jamming en el que se anula la comunicación RF emitiendo ruido suficientemente potente.

Por supuesto, es también posible atacar la información contenida en la etiqueta. Si esta información fuera, por ejemplo, un precio, el atacante podría obtener una rebaja sustanciosa. RF Dump, escrito en Java, y que podía correr en Linux y en Windows XP. Este programa, utilizando un lector RFID conectado al puerto serie del ordenador, leía los datos de la etiqueta y los presentaba en una hoja de cálculo. El usuario puede cambiar datos y volver a escribirlos en la etiqueta.

Otro programa, denominado RF Dump-PDA está escrito en Perl, y corre en PDAs.
Asimismo, son también posibles los ataques al middleware, o incluso al sistema de aplicación, en este caso ataques de tipo “tradicional”, como virus, malware, etc.

Otros tipos de ataque son:

- *Ataques Man in the Middle (MIM)*

Este tipo de ataque se aprovecha de la confianza mutua en el proceso de comunicación suplantando una de las entidades. RFID es particularmente vulnerable a este tipo de ataque, debido a la interoperabilidad de muchos lectores y etiquetas, y a la automatización del proceso de lectura y escritura.

- *Fraudes por modificación de chips*

Lukas Grenwald explica un tipo de ataque realizado sobre una tienda piloto que empleaba etiquetas RFID para marcar cuatro tipos de productos. Utilizando una PDA con un lector RFID pudo leer la información de las etiquetas. Para cerciorarse de que se podían escribir fue al sitio donde se borraba la información de las etiquetas para respetar los aspectos de privacidad y pudo ver que lo que se hacía en ese sitio era reescribir las etiquetas con ceros. Eso le indicó que realmente se podía escribir nueva información en las etiquetas. El paso siguiente fue reescribir la información del tipo y precio de un producto por el tipo y precio de otro mucho más barato, utilizando para ello una PDA, y software estándar de fácil consecución.

- *Inutilización de etiquetas*

Consiste en inutilizar la etiqueta RFID sometiéndola a un fuerte campo electromagnético. Esto se realiza de forma legal cuando compramos un producto y lo acercan a un sistema que desactiva el código de seguridad. Lo que hace este sistema es introducir un pulso electromagnético que inutiliza una sección más débil de la antena, con lo que el sistema queda inoperativo. Si se dispone de la tecnología necesaria, entre otras cosas una antena altamente direccional, se pueden inutilizar las etiquetas de protección de los productos, favoreciéndose así su sustracción.

Por supuesto, existen soluciones que permiten robustecer la seguridad de estos sistemas. Consideraremos a continuación algunas de ellas, sin pretender ser exhaustivos.

Los métodos de autenticación modernos funcionan como en la antigüedad: comprueban el conocimiento de un “secreto” para poder permitir una autenticación segura (por ejemplo conocer una clave criptográfica).

De todos modos se deben implementar algoritmos para prevenir que la clave secreta sea descubierta. Los sistemas de seguridad de los sistemas de RFID deben tener un modo de defensa contra los siguientes ataques individuales:

- La lectura no autorizada de la portadora de la información para poder conseguir una réplica y/o modificar los datos que lleva.
- Colocar una potadora de información extraña en la zona de influencia del interrogador con la intención de obtener un acceso no autorizado a un edificio o a una serie de servicios sin tener que pagarlos.
- Escuchar, sin ser advertido, en las comunicaciones radio y recolocar los datos imitando una portadora original (‘respuesta y fraude’).
- Lecturas/escrituras indeseadas, con objeto de obtener información o modificar datos de forma fraudulenta.

- La existencia de etiquetas falsas dentro de una zona restringida, que tratan de burlar la seguridad del sistema accediendo a lugares no autorizados o recibiendo determinados servicios sin previo pago.
- Escuchas ilegales con objeto de copiar los datos y falsificar etiquetas.

Cuando se selecciona un sistema de RFID para su posterior implementación, debe tenerse en cuenta las medidas de seguridad que necesitan adoptarse dependiendo de su posterior funcionalidad. Así pues, un sistema que pretende una finalidad de automatización industrial o de reconocimiento de herramientas quizás no necesite añadir un costo adicional por medidas de seguridad que sí necesitarán sistemas de alta seguridad como pueden ser los sistemas de pago o de control de acceso a edificios. En el caso de los sistemas que necesitan seguridad, omitir un gasto en un proceso de criptología puede suponer un gasto posterior mucho más elevado si un intruso consigue acceso ilegal a servicios restringidos.

6.2 Aspectos de Privacidad en Sistemas RFID

Otro de los aspectos importantes es el de la privacidad: RFID que hace posible la captura de información personal de forma silenciosa y a veces transparente para el usuario.

Un estudio realizado por Capgemini[1] en 2005 sobre los aspectos de privacidad reveló resultados muy interesantes, que se muestran en la Tabla 2.6. Dicha tabla muestra la opinión del público sobre cómo percibe la privacidad de RFID frente a la privacidad apreciada de otras tecnologías/soluciones tecnológicas. Es decir, los porcentajes de gente que opinan que RFID tiene mayores problemas de privacidad, menores o iguales que las tecnologías con las que se le compara.

Es interesante notar cómo RFID se percibe como causante de un mayor impacto en la privacidad, incluso en comparación con aplicaciones que pueden utilizar RFID, como el control de equipajes o las tarjetas inteligentes, lo que infiere que en realidad se trata de una desinformación o falta de conocimiento de la tecnología RFID. En todos los casos, la apreciación de que RFID tenían menor impacto sobre la privacidad que las tecnologías de comparación fue inferior al 10%. Este resultado muestra la preocupación que puede suscitar en el público el aspecto de la privacidad de los dispositivos RFID, lo cual puede suponer un problema si no se trata con la adecuada prudencia.

[1] http://www.mx.capgemini.com/

RFID Frente a:	Mayor Impacto	Mismo Impacto	Menor Impacto	No sabe / No contesta
Teléfonos Móviles	36	33	10	21
Tarjetas de Debito	36	29	7	26
Tarjetas de crédito	41	31	8	20
Cajeros Automáticos	41	32	8	19
Tarjetas de Compra	42	33	7	18
Control de Equipajes	45	31	6	18
Tarjetas Inteligentes	46	28	6	20
Con Cámara	34	32	10	24

Tabla 6.1 Impacto en la privacidad de RFID frente a otras tecnologías. Fuente: Capgemini

Especialmente relevante para las organizaciones de defensa del consumidor resulta su posible intromisión en la privacidad de las personas, ya que consideran que constituye un medio peligroso para recuperar datos personales sin autorización, sobre todo si se tiene en cuenta que marcas como Gillette, Prada o Benetton la utilizan o la han utilizado ya de manera experimental. Además, si pensamos, por ejemplo, en el uso de RFID como medio de pago, sería sencillo construir un perfil personalizado de los gustos del cliente, con objetivo de presentarle publicidad u ofertas "a medida".

La asociación estadounidense CASPIAN (*Consumers Againts Supermarket Privacy Invasión and Numbering*) lo considera un nuevo medio de intrusión y vigilancia de la vida privada de las personas. Asimismo, en Francia, la CNIL (*Comission Nationale de l'Informatique et des Libertés*) ha calificado la tecnología RFID como de riesgo para las libertades individuales.

Aunque es cierto que la tecnología RFID puede atentar contra la privacidad y confidencialidad de las personas, existen, como ya hemos mencionado, soluciones técnicas para controlar las utilizaciones indeseadas de los sistemas RFID, como son los procedimientos de cifrado y autenticación. El cifrado se utiliza para asegurar que la información sólo pueda ser entendida por los usuarios de la aplicación y evitar de ese modo lecturas indeseadas. La autenticación se utiliza para que únicamente personal autorizado pueda acceder a dicha información, tanto para leer como para escribir.

Los riesgos potenciales hacen surgir un debate, muchas veces acalorado, sobre los aspectos de privacidad

Las asociaciones defensoras de la privacidad insisten en que son necesarias amplias garantías legislativas para asegurar la privacidad antes de la implementación a gran escala de la tecnología RFID a nivel del consumidor. Los principales argumentos que aducen las organizaciones defensoras de la privacidad son los siguientes:

- *Las etiquetas se pueden ocultar con facilidad*. Máxime con la reducción creciente en su tamaño que posibilitan los avances tecnológicos actuales.
- *Cada objeto posee un identificador único*. Lo que posibilita la creación de grandes bases de datos con los gustos de los consumidores. Además, si se relaciona el identificador único con datos personales, se pueden establecer perfiles de los usuarios y realizar un seguimiento de los mismos sin su conocimiento ni su consentimiento.
- *Los lectores se pueden ocultar con facilidad*. Lo que se facilita por la reducción de tamaño y el aumento de la distancia de lectura, tanto en etiquetas activas como pasivas.

Las principales amenazas a la privacidad en los sistemas RFID provienen de:

- *Lecturas no autorizadas de las etiquetas*. Las etiquetas pueden contener información personal, como nombres, fechas de nacimiento, direcciones, etc.

Pueden contener también datos en forma de una clave de acceso a una base de datos con información confidencial sobre las personas.

- *Seguimiento de las personas, preferencias, gustos, etc*. Cuando una persona porta una etiqueta con sus datos y la emplea para pagos de compras, transportes, etc., sus movimientos y gustos pueden ser seguidos y almacenados, extrayendo por ejemplo preferencias y gustos personales.
- *Uso de datos para extracción de información personal*. A partir del conjunto de datos de una persona extraídos del uso de RFID se pueden emplear, por ejemplo, técnicas de minería de datos para encontrar patrones, correlaciones de comportamiento, prioridades, etc., de una persona e incluso de su relación con las demás.
- *Uso de datos para propósitos diferentes de su empleo original*. Una vez se dispone de los datos, nada impide utilizarlos para cualquier propósito.
- *Uso de datos para monitorización de comportamientos específicos*. Esta monitorización se podría realizar en tiempo real, pero también mediante almacenamiento de datos y estudio posterior de los mismos. Por ejemplo, un comerciante podría estudiar los patrones de comportamiento de los usuarios en sus compras para establecer las políticas de precios que le resultaran más ventajosas.

Como respuesta al planteamiento de estos problemas, EPCglobal formó una comisión encargada de buscar el equilibrio entre los aspectos de privacidad y los posibles beneficios de la implantación de la tecnología RFID. Uno de los resultados de esta comisión fueron 4 directrices para la protección de la privacidad de los consumidores. Estas directrices son:

- *Información al consumidor*. Los consumidores deben ser advertidos claramente de la presencia de códigos electrónicos en los productos o envases.

- *Elección del consumidor*. Los consumidores deben ser informados de la elección de un producto de este tipo por si desean descartarlo o quitar las etiquetas RFID.

- *Educación al consumidor*. Los consumidores deben tener la posibilidad de informarse correctamente sobre el uso de las etiquetas electrónicas y sus aplicaciones.

- *Grabación de usos, retención y seguridad*. De la misma forma que con el código de barras, las empresas deben almacenar registros de uso, mantenimiento y protección de la información obtenida con esta tecnología, y deben publicar en sus sitios web sus políticas al respecto.

6.3 Capas de Seguridad en Tarjetas RFID

Para garantizar la seguridad en RFID se ha optado por implementar métodos de seguridad en las diferentes capas de un sistema RFID.

6.3.1 Activación de la seguridad en la capa pasiva

El lector RFID genera ráfagas de energía de diferentes duraciones, el lector genera pulsos con cuatro longitudes de 2, 12, 3, y 9 unidades de tiempo. La etiqueta debe detectar un único código de estas ráfagas a fin de activar el resto de la etiqueta. El sistema basado en el software se aplica con un microprocesador PIC. El sistema basado en hardware es concebido para su aplicación en un ASIC o SoC. La fuerza de la codificación se relaciona con dos componentes: el número de ráfagas n en la secuencia y el número único de diferentes longitudes de ruptura detectable por el receptor b. Así, el número es nb. Los principales componentes del circuito de detección, son dos contadores y una comparación.

El primer contador detecta el valor de la ráfaga determinada por la longitud que requieren de ruptura [lg b] bits y la segunda para realizar el seguimiento de ruptura que se está comprobando en que requieren la secuencia [lg n] bits.

La velocidad de reloj del circuito depende de la precisión de la detección de ruptura del interruptor. Es bajo este proceso que la seguridad en las tarjetas Tags se aplica en su primera fase es decir si la etiqueta detecta mas de una ráfaga de energía transmitida por el lector esta no permite activar el resto de la etiqueta, es decir no proporciona su clave unica en principio por lo tanto no permite la lectura de la misma.

6.3.2 Seguridad en la capa física

Las etiquetas RFID activas en general se comunican a través de algún tipo de codificación Manchester.

La codificación Manchester, también denominada codificación bifase-L, es un método de codificación eléctrica de una señal binaria en el que en cada tiempo de bit hay una transición entre dos niveles de señal. Es una codificación auto sincronizada, ya que en cada bit se puede obtener la señal de reloj, lo que hace posible una sincronización precisa del flujo de datos. Una desventaja es que consume el doble de ancho de banda que una transmisión asíncrona. Hoy en día hay numerosas codificaciones (8B/10B) que logran el mismo resultado pero consumiendo menor ancho de banda que la codificación Manchester.

Descripción de Código Manchester

- Las señales de datos y de reloj, se combinan en una sola que auto-sincroniza el flujo de datos.
- Cada bit codificado contiene una transición en la mitad del intervalo de duración de los bits.
- La primera mitad es el verdadero valor del bit, y la segunda es información que no es necesaria, y simplemente se pone para completar el bit.
-

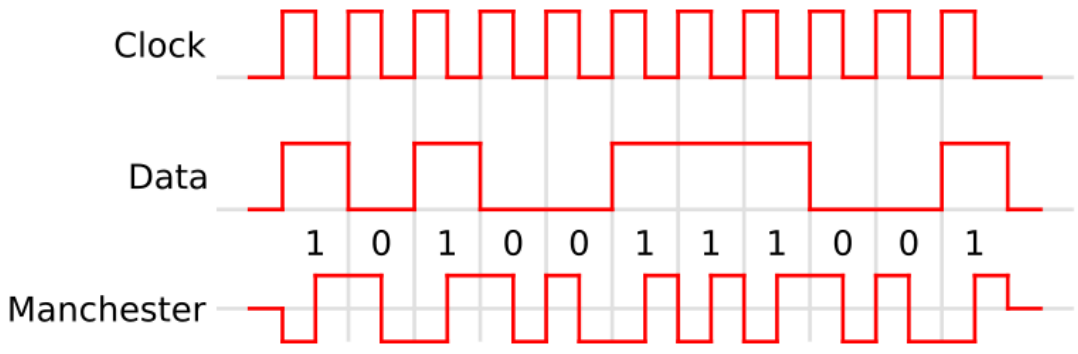


Figura 6.1 Código Manchester

Los códigos Manchester tienen una transición en la mitad del periodo de cada bit. Cuando se tienen bits iguales y consecutivos se produce una transición al inicio del segundo bit, la cual no es tenida en cuenta por el receptor al momento de decodificar, solo las transiciones separadas uniformemente en el tiempo son las que son consideradas por el receptor. Hay algunas transiciones que no ocurren a mitad de bit. Estas transiciones no llevan información útil, y solo se usan para colocar la señal en el siguiente estado donde se llevará a cabo la siguiente transición. Aunque esto permite a la señal auto-sincronizarse, en realidad lo que hace es doblar el requerimiento de ancho de banda, en comparación con otros códigos como por ejemplo los Códigos NRZ.

La codificación Manchester es solo un caso especial de la Modulación por desplazamiento de fase, donde los datos que van a ser transmitidos controlan la fase de una onda rectangular portadora. Para controlar la cantidad de ancho de banda consumida, se puede usar un filtro para reducir el ancho de banda hasta un valor bajo como 1Hz por bit/segundo, y mantenerlo para no perder información durante la transmisión.

Descripción de código Manchester Diferencial

La Codificación Manchester diferencial (también CDP; Conditional DePhase encoding) es un método de codificación de datos en los que los datos y la señal reloj están combinados para formar un único flujo de datos auto-sincronizable. Es una codificación diferencial que usa la presencia o ausencia de transiciones para indicar un valor lógico. Esto aporta algunas ventajas sobre la Codificación Manchester:

- Detectar transiciones es a menudo menos propenso a errores que comparar con tierra en un entorno ruidoso.
- La presencia de la transición es importante pero no la polaridad. La codificaciones diferenciales funcionaran exactamente igual si la señal es invertida (cables intercambiados).

Un bit '1' se indica haciendo en la primera mitad de la señal igual a la última mitad del bit anterior, es decir, sin transición al principio del bit. Un bit '0' se indica haciendo la primera mitad de la señal contraria a la última mitad del último bit, es decir, con una transición al principio del bit. En la mitad del bit hay siempre una transición, ya sea de high hacia low o viceversa. Una configuración inversa es posible, y no habría ninguna desventaja en su uso.

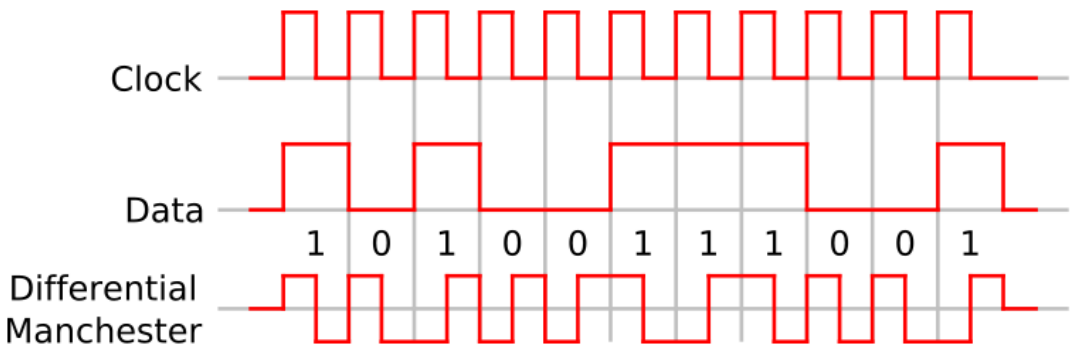


Figura 6.2 Código Manchester Diferencial

Un método relacionado es la Codificación Manchester en el cual las transiciones significativas son las de la mitad del bit, codificando los datos por su dirección (positivo-negativo es valor '1', negativo-positivo es el otro).

A fin de proteger los datos los fabricantes de tarjetas RFID han optado por combinar el uso de los códigos Manchester y del diferencial Manchester en la misma secuencia.

Para convertir Manchester o Manchester diferencial de código de bits en vectores, la señal es la muestra para detectar la transición en el medio o al principio de la ventana, respectivamente.

6.3.3 Seguridad física

Las etiquetas RFID son desplegadas a menudo en entornos que no ofrecen seguridad física al dispositivo. Esto expone a la etiqueta RFID a una clase de ataques que implican el análisis e implementación de técnicas para determinar la clave secreta almacenada en el dispositivo, por personas malintencionadas. Estos tipos de ataques de energía han sido eficaces para romper el cifrado de las tarjetas inteligentes. La primera clase de ataque es SPA (Simple Power Analysis, que implica la correlación de consumo de energía en el dispositivo para que “entregue” su clave secreta.

La segunda clase de ataque es el DAP (Diferencial Power Análisis), el cual utiliza el análisis estadístico para ayudar a descubrir la clave secreta [10]. Mientras tanto SPA y DPA exigen el conocimiento del comportamiento del algoritmo de encriptación, SPA sólo es eficaz cuando el algoritmo tiene un control de flujo que depende de la clave secreta, por lo que es un ataque mucho más potente.

Los ataques DPA intentan descubrir la clave secreta dividiendo la clave en los subgrupos de un número limitado de bits y huellas para poder examinar todas las combinaciones de cada uno de

estos subgrupos. Por ejemplo, en 128-bit AES, la clave de 128 bits se subdivide en 32 grupos de 4 bits cada una. Durante el DAP, un subgrupo se examina entre"0000"y"1111" y pone un número fijo al resto de los subgrupos.

El método DPA consta en comparar una clave secreta de una tag RFID con un conjunto de claves aleatorias

Cabe destacar que la seguridad en las instalaciones donde se utilicen sistemas RFID debe ser de alto nivel en todos los sentidos desde llevar un control de acceso a las instalaciones para evitar que personas malintencionadas entren con fines malintencionadas hasta la destrucción de los tags desechados por los sistemas pasando por hacer las configuraciones necesarias en el hardware del sistema RFID y el equipo de computo así como el blindaje de las redes informáticas y el control de acceso al equipo de computo donde se gestiona la información proporcionada por las tags como pueden ser ordenados, servidores, lectores, programadores u otros.

6.4 Criptografía utilizada en Sistemas RFID

En esta sección, se discuten los planes de protección de privacidad de RFID que utilizan una función del algoritmo hash, que es una función criptográfica de peso ligero, y puede ser computada dentro de la etiqueta RFID.

En estos sistemas, una etiqueta RFID calcula la función de hash en su interior para proteger su contenido.

El lector tiene la clave K para cada marca, y cada etiqueta tiene valor hash h ¼ H (k), llamado meta-ID, donde H es la función de hash. Una etiqueta que recibe una solicitud de ID de acceso y los envía meta-ID h en respuesta. El lector envía clave k que se refiere a la meta-ID recibido h de la etiqueta. La etiqueta calcula la función de hash de la clave k recibidas y los controles la relación de h ¼ H (k) con meta-ID. La etiqueta responde con su propio ID al lector sólo si tiene la relación.

Sin embargo, el método sigue siendo susceptible a posibles ataques ya el algoritmo de hash es un algoritmo difícil de descifrar y muy ligero por lo mismo muchos atacantes desarrollan técnicas avanzadas para tratar de desencriptar dicho algoritmo.

Por tal motivo han surgido dos técnicas importantes para contrarrestar lo mencionado con anterioridad, la criptografía de clave secreta y publica y el algoritmo DES (Data Encryption Standard) y el algoritmo IDE ((International Data Encription Algorithm).

6.4.1 Criptografía de clave secreta o simétrica

Los criptosistemas de clave secreta o Simétrica se caracterizan porque la clave de cifrado y la de descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Sus principales características son:

- Rápidos y fáciles de implementar
- Clave de cifrado y descifrado son la misma
- Cada par de usuarios tiene que tener una clave secreta compartida
- Una comunicación en la que intervengan múltiples usuarios requiere muchas claves secretas distintas

Actualmente existen dos métodos de cifrado para criptografía de clave secreta, el cifrado de flujo y el cifrado en bloques.

6.4.1.1 Cifrado de flujo

El emisor A, con una clave secreta y un algoritmo determinístico (RKG), genera una secuencia binaria (*s*) cuyos elementos se suman módulo 2 con los correspondientes bits de texto claro *m*, dando lugar a los bits de texto cifrado *c*, Esta secuencia (*c*) es la que se envía a través del canal. En recepción, B, con la misma clave y el mismo algoritmo determinístico, genera la misma secuencia cifrante (*s*), que se suma modulo 2 con la secuencia cifrada (*c*), dando lugar a los bits de texto claro *m*.
Los tamaños de las claves oscilan entre 120 y 250 bits:

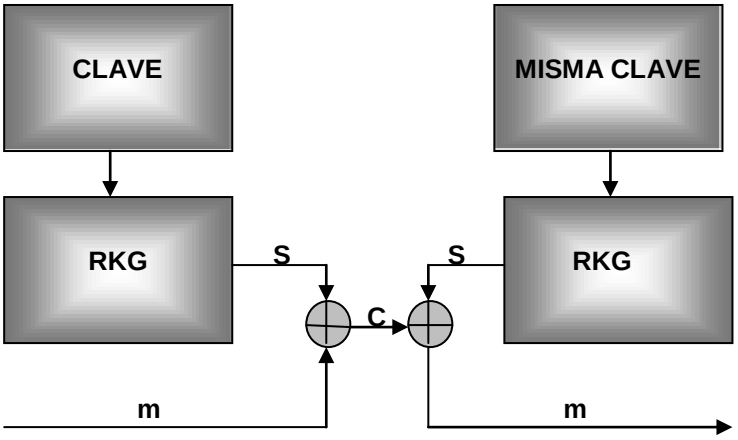


Figura 6.3 Ejemplo del diagrama de bloques del cifrado de flujo.

6.4.1.2 Cifrado en bloque

Los cifrados en bloque se componen de cuatro elementos:

- Transformación inicial por permutación.
- Una función criptográfica débil (no compleja) iterada r veces.
- Transformación final para que las operaciones de encriptación y desencriptación sean simétricas.
- Uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total.

6.4.1.3 Cifrado de Feistel

Se denominan así los criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja, alternativamente, con una de las mitades. Pertenecen a este tipo los criptosistemas LUCIFER, DES, LOKI y FEAL.

6.4.1.4 Algoritmo DES (Data Encryption Standard)

El algoritmo DES surge como consecuencia de un concurso organizado por NBS (National Bureau of Standards, USA) el cual solicitaba un “algoritmo de encriptación para la protección de datos de ordenador durante su transmisión y almacenaje”. Este concurso lo ganó IBM con su algoritmo DES (modificado del LUCIFER) [28]

DES es un algoritmo de cifrado en bloque; la longitud de bloque es de 64 bits (8 símbolos ASCII); la longitud de la clave es de 56 bits, lo que equivale a que existan:

256 = 7,2 • 1016 claves diferentes

La norma del DES es FIPS (Federal Information Processing Standards). La norma exige que el DES se implemente mediante un circuito integrado electrónico. El chip de DES es un producto estratégico USA. No está permitida su exportación sin un permiso especial, y no se permite comercializar en USA chips fabricados en el exterior.

El ANSI (American National Standards Institute, USA) adopta el DES con el nombre de DEA (Data Encryption Algorithm) el cual no exige la implementación del algoritmo en un chip, pudiendo ser programado mediante software. Las librerías de implementación de DES y DEA son openSSL.

Estructura del DES

El DES trabaja alternativamente sobre las dos mitades del bloque a cifrar. En primer lugar se hace una permutación. Después se divide el bloque en dos mitades, a continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar módulo 2 la parte izquierda con la función *F (Ki)* de la derecha, gobernada por una subclave *Ki.*

Después se intercambian las partes derecha e izquierda. En la vuelta 16 se remata el algoritmo con una permutación final que es la inversa de la inicial.

Para descifrar el DES basta con repetir la operación modular, es decir, su aplicación repetida dos veces conduce a los datos originales.

Función F (Ki)

Las operaciones realizadas por la función F son:

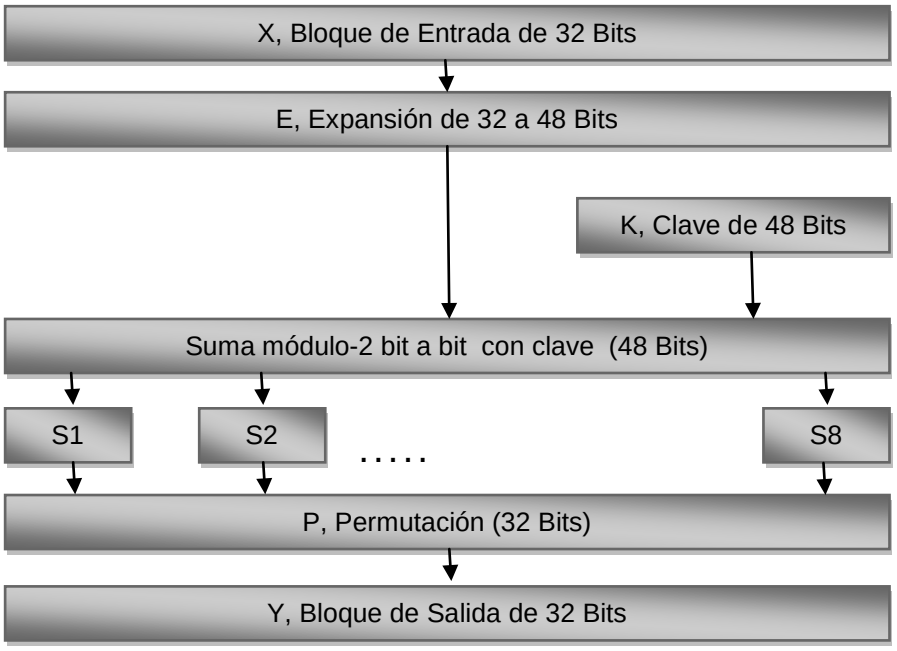


Figura 6.4 Operaciones realizadas por la función F.

Lo primero que se hace es fabricar un vector de 48 bits a partir de los 32 bits iniciales a través de una expansión lineal. Esta expansión es la que se describe a continuación:

Izquierda	32	1	2	3	4	5	4	5	7	8	9
Centro Izquierda	8	9	10	11	12	13	12	13	15	16	17
Centro Derecha	16	17	18	19	20	21	20	21	23	24	25
Derecha	24	25	26	27	28	29	28	29	31	32	1

Tabla 6.2 Ejemplo de la expansión lineal usada

Después se combina la clave local de 48 bits con la expansión por suma módulo 2 bit a bit, obteniéndose un vector de 48 bits que se divide en 8 grupos de 6 bits. Cada grupo entra en las llamadas “cajas S”. Estas cajas son las responsables de la *no linealidad del DES*. En cada caja entran 6 bits, pero salen únicamente 4 bits. Además los bits centrales se sustituyen en función de los bits laterales. Los principios para la elección de las cajas S no han sido revelados y es información clasificada por el gobierno de los Estados Unidos.

La caja P realiza una permutación lineal fija, esta permutación es la siguiente:

El bloque	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
Se cambia por:	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Tabla 6.3 Ejemplo de la permutación lineal fija usada

Expansión de claves Ki

En DES se manejan claves de 64 bits, pero se le realiza una operación de reducción a 56 bits, eliminando un bit de cada ocho. A continuación se reordenan los bits restantes mediante una permutación fija que carece de significación criptográfica.

Después se generan las 16 subclaves necesarias en las 16 vueltas del algoritmo. Cada subclave estará compuesta por 48 bits.

La forma de generar las subclaves es la siguiente:

- Se divide la clave de 56 bits en dos mitades de 28.
- Cada mitad se rota a la izquierda uno o dos bits dependiendo de la vuelta (de 1 a 16).
- Después de las rotaciones se vuelven a unir las mitades teniendo 16 grupos de 56 bits.
- A continuación se realiza una “permutación con compresión”. Esta permutación elige 48 bits de cada grupo formando así las 16 subclaves.

Modos de uso

En la norma ISO 8372 se definen cuatro modos de uso de cualquier cifrado en bloque:

- ECB (Electronic Codebook): se caracteriza por el uso directo de un cifrador en bloque.
- CBC (Cipher Block Chaining): se carga inicialmente el registro (64 bits) con un vector inicial (VI) que no importe que sea secreto, pero si aleatorio. Sus principales características son que convierten el DES en un cifrador en flujo y puede hacer que cifre mensajes iguales de forma diferente con solo cambiar cada vez el VI.

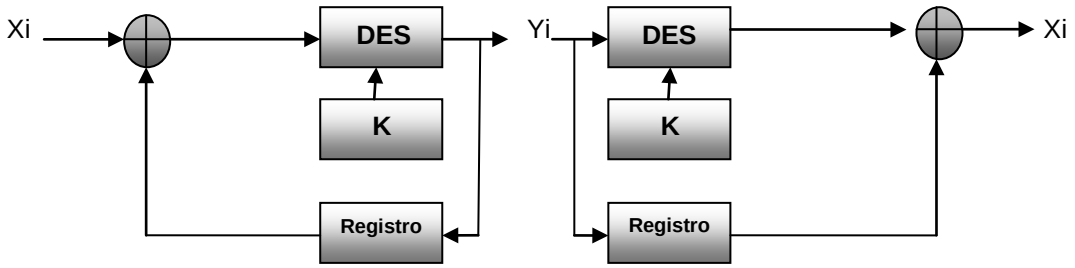


Figura 6.5 Diagrama de bloques del cifrado Cipher Block Chaining CBC

- CFB (Cipher Block Chaining): se carga inicialmente el registro de desplazamiento de 64 bits con un vector inicial (VI) que no importa que sea secreto, pero si aleatorio. Se divide el mensaje en claro en bloques de n bits. La operación de suma módulo 2 se hace bit a bit sobre bloques de n bits que pueden variar de 1 y 64. El registro de desplazamiento de 64 bits se desplaza a la izquierda n bits después de cada operación de cifrado de cada bloque.

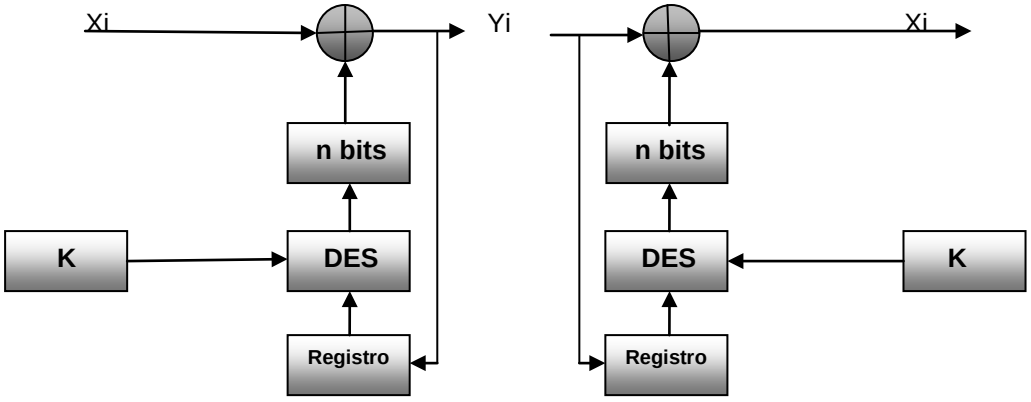


Figura 6.6 Diagrama de bloques del Cipher Block Chainig CFB

- OFB (Output Feedback): el funcionamiento es igual que en CFB, pero ahora el VI si tiene que ser secreto. Su principal característica es que convierte el DES como un generador de secuencia cifrante.

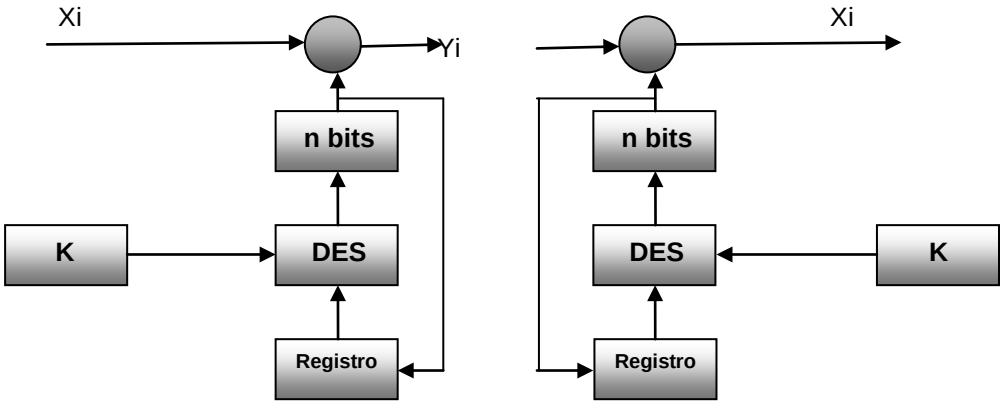


Figura 6.7 Diagrama de bloques del Output Feedback

Cifrado triple

Es un modo de cifrado para el DES o cualquier otro cifrador en bloque que no llega a ser un cifrado múltiple, porque no son independientes todas las subclaves. Es inmune a un ataque por encuentro a medio camino. Para el DES la longitud efectiva de clave es de 112 bits.

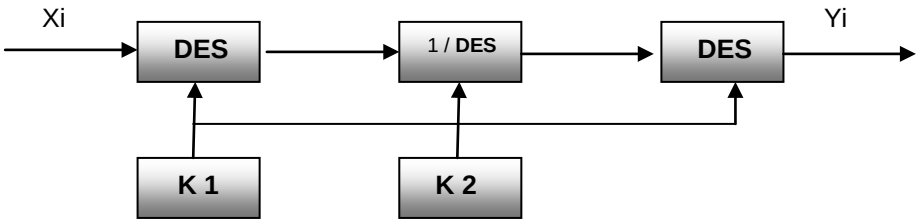


Figura 6.8 Diagrama de bloques del cifrado triple

6.4.1.5 IDEA (International Data Encryption Algorithm)

En el algoritmo Internacional de Cifrado de Datos, tanto los datos en claro como los cifrados están compuestos por bloques de 64 bits, mientras que la clave consta de 128 bits. Se basa en el concepto de mezclar operaciones aritméticas de grupos algebraicos diferentes (introduce confusión y difusión en el mensaje) [29] Se realizan ocho vueltas de encriptación idénticas seguidas de una transformación de salida. Es decir, como el DES, pero las vueltas son más complejas. En cada vuelta de encriptación, el bloque de datos de entrada es dividido en cuatro sub-bloques de 16 bits. A su vez se utilizan para cada vuelta seis subclaves.

Este algoritmo es muy seguro porque:

- Claves 2128 no se pueden computar actualmente.
- No se le puede aplicar criptoanálisis diferencial a partir de la cuarta vuelta, y este tiene ocho.
- Como inconveniente tiene que si se deducen varios sub-bloques de la clave, se puede deducir la clave.

6.4.2 Criptografía de clave pública o asimétrica

En la criptografía de clave secreta se presentan los siguientes problemas:

- **Distribución de claves**. Dos usuarios tienen que seleccionar una clave en secreto antes de empezar a comunicarse, lo que deberá hacer bien personalmente (cosa que no siempre es posible), bien por medio de un canal inseguro.

- **Manejo de claves**. En una red de n usuarios, cada pareja debe tener su clave secreta particular, lo que hace un total de n(n-1)/2 claves para esa red.
- **Sin firma digital**. En los criptosistemas de clave secreta no hay posibilidad, en general, de firmar digitalmente los mensajes, con lo que el receptor del mismo no puede estar seguro de que quien dice que le envía el mensaje sea realmente quien lo ha hecho. De todos modos, este punto afecta poco a los sistemas RFID ya que no contienen firma digital.

6.4.2.1 Cambio de clave de Diffie-Hellman

Para evitar los problemas que se acaban de mencionar, Diffie y Hellman describieron un protocolo por medio del cual dos personas pueden intercambiarse pequeñas informaciones secretas por un canal inseguro. Es el siguiente:

1. Los dos usuarios *A* y *B*, seleccionan un grupo multiplicativo finito *G*, de orden *n* *(Zn*)* y un elemento $\alpha \in G$ (generador).
2. *A* genera un número aleatorio *a*, calcula $\alpha^a \pmod n$ en *G* y transmite este elemento a *B*
3. *B* genera un número aleatorio *b*, calcula $\alpha^b \pmod n$ en *G* y transmite este elemento a *A*

4. *A* recibe α^b y calcula $(\alpha^b)^a$ en *G*
5. *B* recibe α^a y calcula $(\alpha^a)^b$ en *G*

Ejemplo: Sea *p* el número primo 53. Supongamos que *G=Z53 * = {1,2,...,52}* y sea $\alpha = 2$ un generador. El protocolo Diffie-Hellman es el siguiente:

1. *A* elige *a*=29, calcula $\alpha^a = 229 \equiv 45 \pmod{53}$ y envía 45 a *B*.
2. *B* elige *b*=19, calcula $\alpha^b = 219 \equiv 12 \pmod{53}$ y envía 12 a *A*.
3. *A* recibe 12 y calcula $1229 \equiv 21 \pmod{53}$.
4. *B* recibe 45 y calcula $4519 \equiv 21 \pmod{53}$

Ahora una escucha conocerá *Z53 **, 2, 45 y 12, pero no puede conocer la información secreta compartida por A y B que es 21.

6.4.2.2 Algoritmo asimétrico ELGAMAL

Supongamos que los mensajes son elementos de G y que el usuario A desea enviar un mensaje m al usuario B. El protocolo utilizado es el siguiente:

1. Se selecciona un grupo finito G y un elemento α de G.

2. Cada usuario A elige un número aleatorio a, que será su clave privada, y calcular αa en G, que será su clave pública.

Para que un usuario A envíe un mensaje, *m*, a otro usuario B, suponiendo que los mensajes son elementos de G, realiza las siguientes operaciones:

1. A genera un número aleatorio *v* y calcula αv en G
2. A mira la clave pública de B, αb, y calcula (αb)v y *m* • αbv en G
3. A envía la pareja (αv, *m* • αbv) a B

Para recuperar el mensaje original:

1. B calcula(αv)b en G
2. B obtiene *m* sólo con calcular □ *m* • αbv / αvb

6.5 Control de Errores

Cuando se usa el canal móvil para transmitir señales con información útil existe un riesgo muy elevado de pérdida de información si no se implementan métodos que eviten en cierta medida, los errores de transmisión.

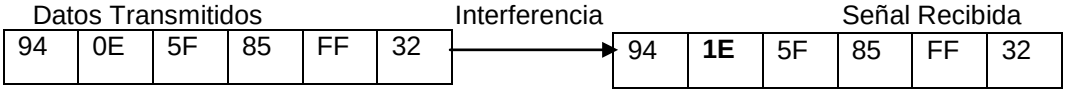


Figura 6.9 Las interferencias durante la transmisión pueden generar errores en los datos transmitidos.

El control de errores se usa para reconocer errores en la transmisión e iniciar medidas de corrección como, por ejemplo, pedir la retransmisión de los bloques de datos erróneos. Las medidas más comunes de control de errores son el control de paridad, la suma XOR y el CRC.

Control de paridad

El control de paridad es un muy sencillo y común método para realizar un control de errores eficaz. Este método incorpora un bit de paridad en cada byte transmitido, con un resultado de 9 bits enviados por cada byte de información.

Antes de la transmisión de datos debe tener lugar una decisión para dirimir si se establece una paridad par (even) o impar (odd) para asegurarnos de que emisor y receptor realizan el control de acuerdo con una misma selección. El valor del bit de paridad es fijado de modo que si usamos una paridad par, un número par de '1' debe contarse en los nueve bits. Por otro lado, si la paridad es

impar, un número impar de ‘1’ debe poder contarse en los nueve bits. La paridad impar puede ser también interpretada como el control horizontal (módulo 2) de los bits de datos. Este control horizontal también permite el cálculo de los bits de datos usando puertas lógicas OR exclusivas (XOR).

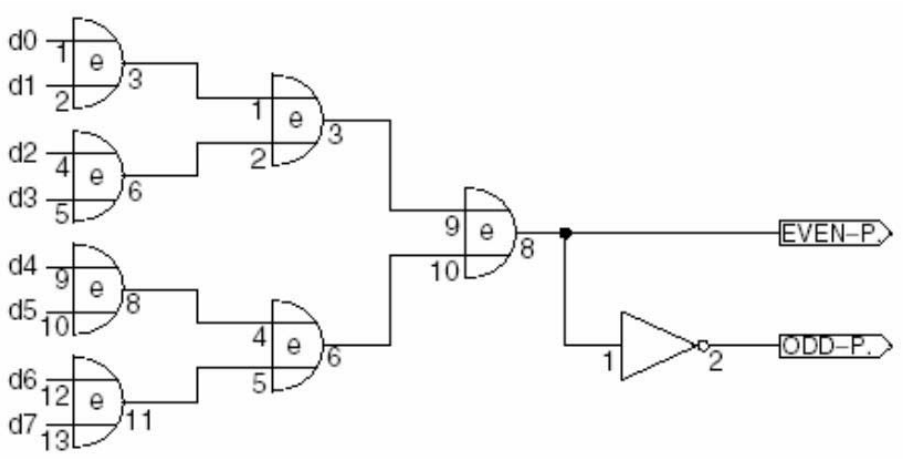


Figura 6.10 El bit de paridad puede ser hallado usando múltiples puertas XOR y realizando operaciones bit a bit.

De todos modos, la simplicidad de este método está contrarrestada por su pobre reconocimiento de errores (Pein, 1996). Si existe un número impar de bits erróneos (1,3,5,7) siempre serán detectados, mientras que si el número de bits erróneos es par (2, 4, 6,
8), unos errores cancelan a los otros y la paridad aparece como correcta.

Método LRC

La suma de comprobación XOR, conocida como control de redundancia longitudinal (*LRC – Longitudinal redundancy checksum*) puede ser calculado rápida y fácilmente.

La suma de comprobación XOR se genera mediante el puerteo XOR recursivo de todos los bytes de datos en un solo bloque de datos. El byte 1 se pasa por una XOR con el byte 2, la salida de esta OR exclusiva es pasado por una XOR con el byte 3, etcétera. Si el resultado del LRC se añade al bloque de datos que se transmite, entonces un simple control de la transmisión una vez es recibida puede detectar los errores. El método a seguir es generar una suma LRC de todos los bytes recibidos (bloque de datos + resultado LRC añadido). El resultado de esta operación debe ser siempre cero; cualquier otro resultado nos indica que ha habido errores en la transmisión.

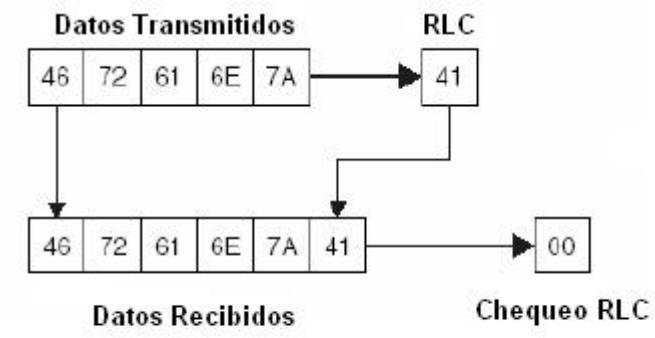


Figura 6.11 Si el LRC es añadido a los datos a transmitir, entonces un nuevo cálculo del LRC de los campos de datos recibido debe resultar 00h (la h indica que trabajamos con números hexadecimales). Esto permite una rápida verificación de los datos sin necesidad de conocer el actual valor de LRC.

Debido a la simplicidad de este algoritmo, los LRCs pueden ser calculados muy simplemente y rápidamente. De todos modos, los LRCs no son muy fiables porque es posible que múltiples errores se cancelen los unos a los otros y lograr así que el control no pueda detectar si se han transmitido con el bloque de datos. Los LRC son usados básicamente para el control rápido de bloques de datos muy pequeños (32 bytes, por ejemplo).

Método CRC

El CRC (Control de redundancia cíclica) fue originalmente usado en controladores de disco. La gran ventaja es que puede generar una suma de comprobación suficientemente segura para grandes cantidades de datos.

Se puede decir que es un excelente control de errores tanto para transmisiones vía cable (por ejemplo por vía red telefónica) como para radiocomunicaciones inalámbricas (radio, RFID). De todos modos, aunque el control de redundancia cíclica representa un método muy seguro para reconocer errores, tiene una pega: no puede corregirlos.

Como su propio nombre sugiere, el cálculo del CRC es un proceso cíclico**.** Así, el cálculo del valor del CRC de un bloque de datos incorpora el valor del CRC de cada uno de los bytes de datos. Cada byte de datos individual es consultado para obtener el valor del CRC del todo el bloque de datos entero.

Matemáticamente hablando, un CRC es calculado dividiendo los datos entre un polinomio usando un llamado *generador de polinomios.* El valor del CRC es el resto obtenido de esta división. Para ilustrar mejor esta explicación, la figura que viene a continuación nos muestra el cálculo de un CRC de 4 bits para un bloque de datos. El primer byte del bloque de datos es 7Fh y el generador de polinomios es x4 + x + 1 = 10011:

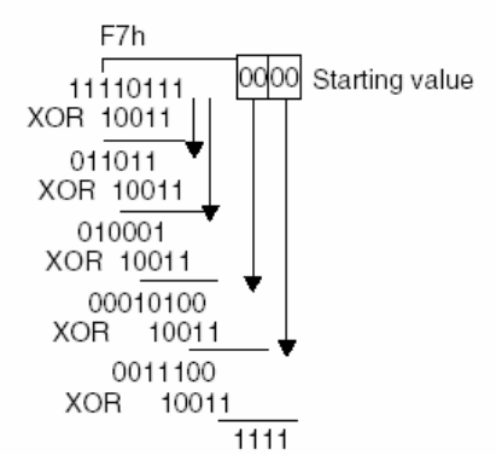


Figura 6.12 Paso a paso del cálculo de un CRC.

Si un CRC que acaba de ser calculado se anexa al final del bloque de datos y se realiza un nuevo cálculo del CRC, el nuevo valor calculado resultará ser cero. Esta característica particular del algoritmo del CRC es explotada para calcular errores en transmisiones de datos en serie.

Cuando un bloque de datos es transmitido, el valor del CRC de los datos es calculado por el transmisor, anexado al final del dicho bloque y transmitido con él. Una vez el bloque de datos es recibido, el receptor calcula el valor del CRC de todo el bloque de datos de modo que, por la propiedad que hemos mencionado anteriormente, el resultado que debe obtener es cero a no ser que exista errores en la transmisión.

Buscar el cero en el CRC del receptor es un método sencillo y rápido de poder comprobar la validez de los datos recibidos. Si no usáramos este método, deberíamos calcular el CRC del bloque de datos útil (es decir, de la información enviada quitándole los últimos bits de CRC) y después comparar el valor obtenido con el CRC recibo, lo que supone un proceso mucho más costoso que realizar el CRC de todo el bloque y buscar un resultado que sea cero.

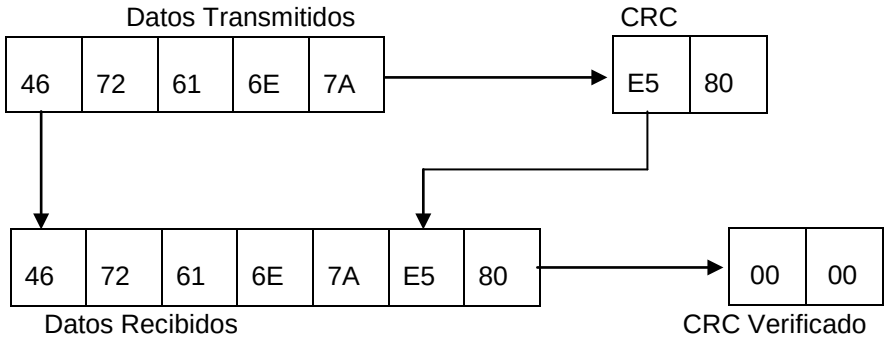


Figura 6.13 Si el valor del CRC se coloca al final del bloque de datos y se transmite todo junto. Al calcular de nuevo el CRC, esta vez de todo el bloque recibido, el resultado debe ser cero; sino existe algún error en la transmisión.

La gran ventaja que presenta el cálculo del CRC es su gran eficacia a la hora de reconocer la existencia de errores realizando un pequeño número de cálculos, incluso cuando existen múltiples errores.
Un CRC de 16 bits es capaz de reconocer los errores de bloques de datos que se encuentran por encima de los 4Kbytes. Un sistema de RFID transmite bloques de menos de 4Kbytes, por lo que los CRC usados pueden incluso ser menores de 16 bits.

A continuación tenemos unos ejemplos de generadores polinomiales:

CRC-8	$x^8+x^4+x^3+x^2+1$
CRC-16 / (controlador de disco)	$x^{16}+x^{15}+x^2+1$
CRC-16 /CCITT	$x^{16}+x^{12}+x^5+1$

Tabla 6.4 Generadores polinomiales

6.6 Multiacceso: Anticolisión

Muchas veces un sistema de RFID tiene numerosos transponders dentro de su zona de interrogación. En este tipo de situación podemos diferenciar entre 2 principales tipos de comunicación.

La primera es usada para transmitir datos desde el lector a la etiqueta (como vemos en la Figura 6.14, que tenemos a continuación). El flujo de datos enviado es transmitido por todos tags simultáneamente (similar a miles de equipos de radio que reciben la señal desde una estación base). Este tipo de comunicación es la que conocemos como *broadcast*.

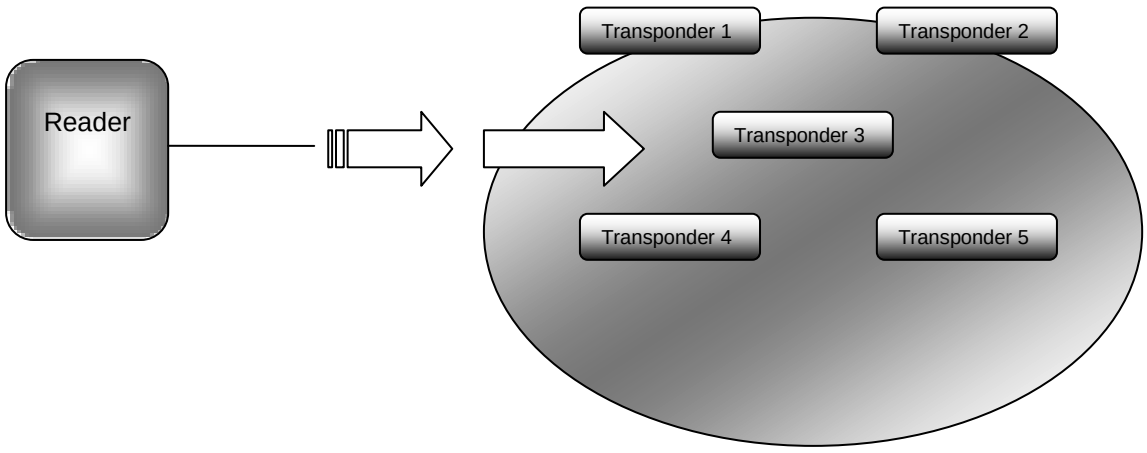


Figura 6.14 Modo broadcast: el flujo de datos transmitido por el lector es recibido simultáneamente por todas las etiquetas que se encuentran en la zona de interrogación.

La segunda forma de comunicación supone la transmisión de datos desde muchas etiquetas, que se encuentran en la zona de interrogación, hacia el lector. Esta forma de comunicación es llamada *multiacceso.*

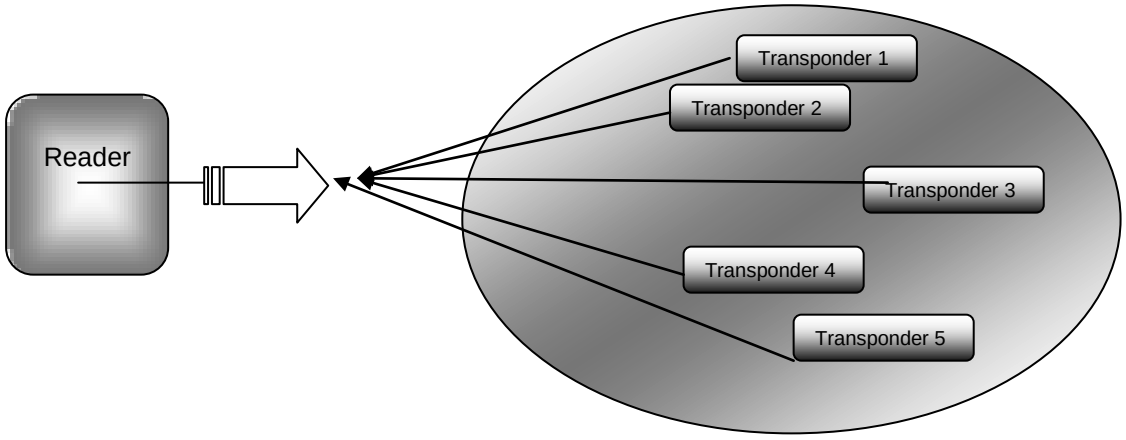


Figura 6.15 Multiacceso: múltiples tags se comunican a la vez con el lector.

Cada canal de comunicación tiene definida la capacidad de canal, la cual es determinada por el ratio máximo de transferencia de dicho canal de comunicación y el tiempo que está disponible.

La capacidad de canal disponible debe ser dividida entre cada participante (etiqueta) y el resultado será la cantidad que puede transmitir cada tag al mismo lector sin que sufran interferencias unos por culpa de los otros (colisión).

El problema del multiacceso ha existido desde hace mucho tiempo en la tecnología radio. Como ejemplo podemos fijarnos en los satélites o en las redes de telefonía móvil donde un gran número de participantes intenta acceder a un mismo satélite o estación base.

Por este motivo han sido desarrollados numerosos métodos con el objetivo de separar la señal de cada participante individual de la de otro cualquiera. Básicamente existen 4 métodos diferentes: acceso múltiple por división de espacio (*space división multiple access, SDMA)*, acceso múltiple por división de frecuencia (*frequency domain multiple access, FDMA)*, acceso múltiple por división de tiempo (*time domain multiple access, TDMA*), y acceso múltiple por división de código (*code division multiple access, CDMA)*; esta última también conocida como técnica del espectro ensanchado (*spread spectrum*).

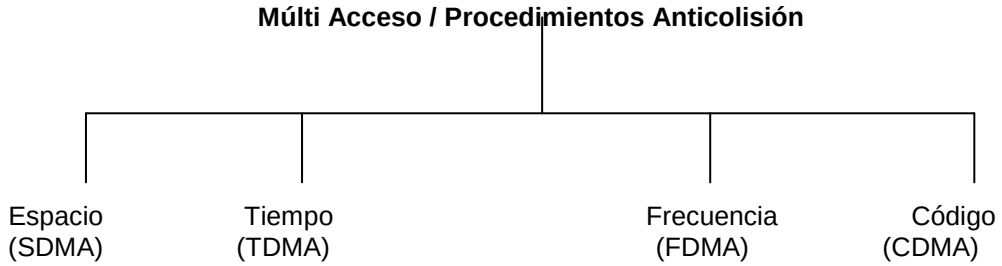


Figura 6.16 Los métodos de multiacceso están divididos en cuatro métodos básicos.

De todos modos, estos métodos clásicos están basados en la suposición de un flujo de datos continuo e interrumpido desde y hacia los participantes. En el momento que se dedica una capacidad de canal, dicha capacidad permanece dedicada hasta que termina la comunicación (p.e. mientras dura una llamada telefónica).
Por otro lado las etiquetas de un sistema RFID se caracterizan por periodos de actividad, intercalados con periodos de inactividad de distinta duración. La capacidad del canal tan sólo se dedica durante el tiempo justo y necesario para establecer un intercambio de datos.
En el contexto de los sistemas RFID, el proceso técnico (protocolo de acceso) que facilita el manejo de múltiples accesos, evitando así las interferencias, es llamado *sistema anticolisión*.

Por motivos de competencia, los fabricantes de sistemas no ofrecen al público los sistemas anticolisión que usan. A continuación vamos a describir los métodos multiacceso que son frecuentemente usados con el fin de ayudar a comprender los métodos anticolisión y, finalmente, expondremos algunos ejemplos de los mismos.

6.6.1 Técnica de Acceso múltiple por división de espacio (SDMA)

El término *acceso múltiple por división de espacio* se refiere a técnicas que rehúsan un cierto recurso (capacidad de canal) en áreas espaciales separadas.

Una opción es reducir significativamente el área de lectura de un único lector, pero para compensarlo entonces se tiene que situar un gran número de lectores y antenas en forma de array de manera que cubran toda el área que antes cubría el lector cuando tenía más alcance.

Otra opción es usar una antena direccionable eléctricamente en el lector. De este modo se puede apuntar a los tags directamente (SDMA adaptativo). De este modo varias etiquetas pueden ser diferenciadas por su posición angular en la zona de interrogación del lector (si el ángulo entre dos transponders es mayor que el ancho de haz de la antena direccional usada, un mismo canal puede ser usado varias veces).

Esto consiste en un grupo de dipolos que forman la antena; por esto mismo el SDMA adaptativo sólo se puede usar en aplicaciones RFID con frecuencias por encima de los 850MHz. Si se usaran frecuencias menores el tamaño de los dipolos sería excesivamente grande. Cada uno de los dipolos está colocado de manera que tiene una fase independiente de los demás dipolos.

El diagrama de radiación de la antena se halla mediante la superposición de los diferentes diagramas de radiación de los dipolos situados en diferentes direcciones.

Para fijar la dirección, los dipolos están alimentados por una señal de alta frecuencia de fase variable, regulada por unos controladores de fase.

Con la intención de cubrir todo el espacio, se deberá escanear el área de interrogación usando la antena direccional hasta que una etiqueta sea hallada dentro del foco de búsqueda del lector.

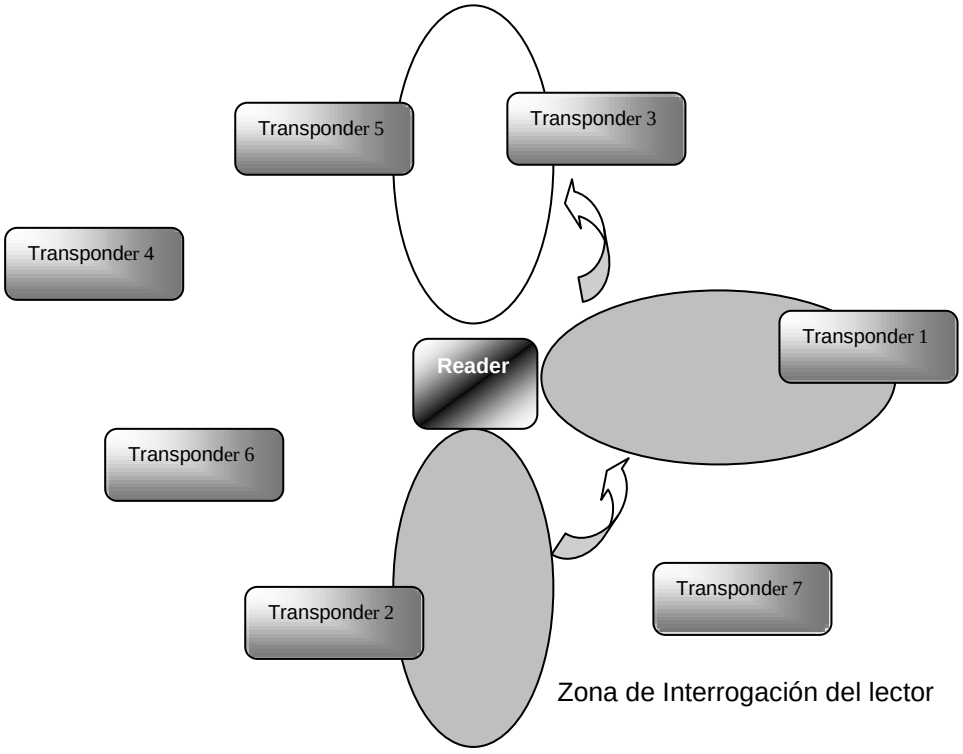


Figura 6.17 SDMA adaptativo con una antena direccionable eléctricamente. El ancho de haz es diseccionado a varias etiquetas; una tras la otra.

Un inconveniente del SDMA es el relativamente alto costo de implementación debido al complicado sistema de la antena. El uso de este tipo de técnica anticolisión queda restringida a unas pocas aplicaciones especializadas.

6.6.2 Técnica de Acceso múltiple por división de frecuencias (FDMA)

El término *acceso múltiple por división de frecuencias* se refiere a las técnicas en las cuales varios canales de transmisión con varias frecuencias portadoras, están disponibles para los participantes en la comunicación

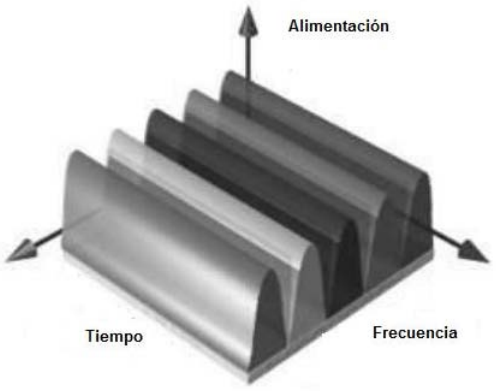


Figura 6.18 En FDMA se tiene varios canales frecuenciales en el mismo instante de tiempo.

En los sistemas RFID esto puede ser logrado una frecuencia de transmisión no harmónica y ajustable libremente. Pueden ser usados varios canales dentro de los rangos de frecuencia definidos por las especificaciones para realizar la transmisión. Esto puede conseguirse usando varias subportadoras de diferente frecuencia cada una. La figura 6.19 hace referencia a lo anteriormente mencionado.

Uno de los inconvenientes de los sistemas que usan FDMA es el costo relativamente elevado que supone para realizar los lectores ya que desde un receptor dedicado tiene que ser posible la recepción para cada canal.

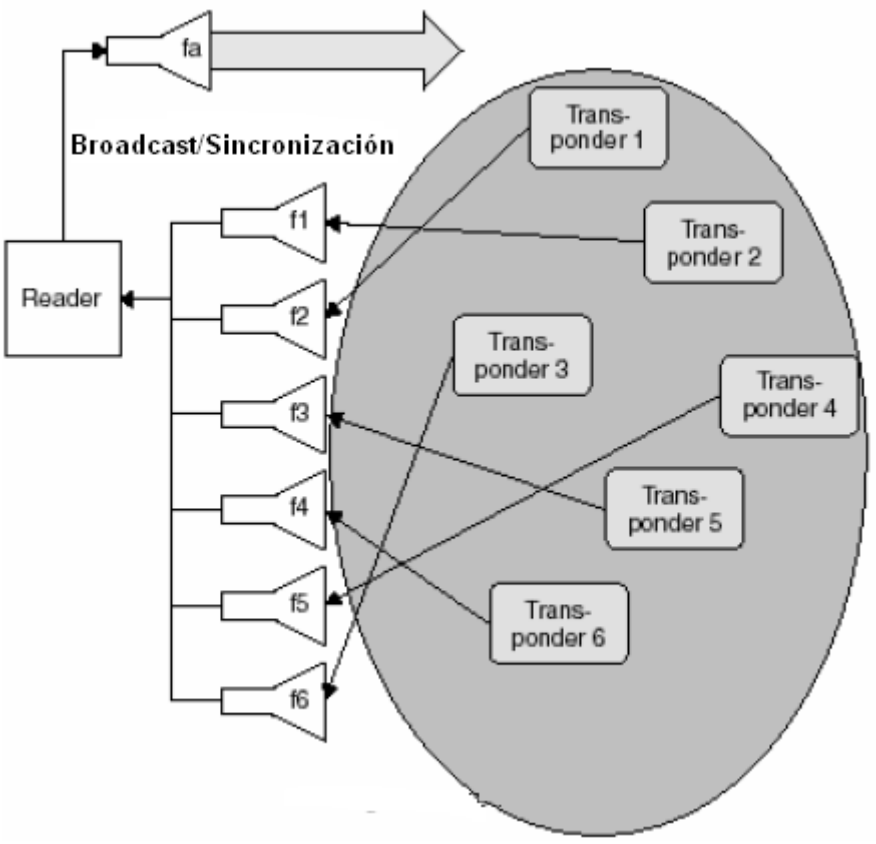


Figura 6.19 Uso de diferentes subportadoras

6.6.3 Técnica de Acceso múltiple por división de tiempo (TDMA)

El término *acceso múltiple por división de tiempo* se refiere a las técnicas de multiacceso en las cuales un canal disponible es dividido cronológicamente entre todos los participantes de la comunicación. El uso de TDMA está particularmente extendido en el campo de los sistemas digitales de radiocomunicaciones móviles.

En los sistemas RFID, TDMA es, de largo, el método usado en un mayor número de técnicas anticolisión.

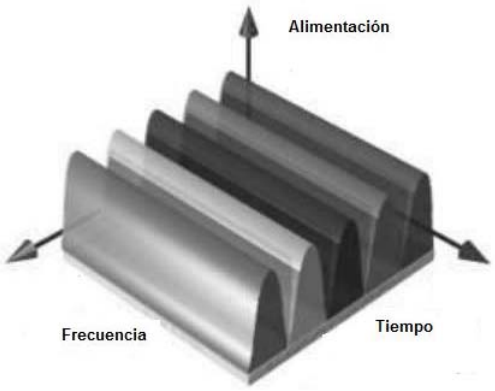


Figura 6.20 En TDMA se usa todo al ancho de banda disponible del canal, repartiéndolo cronológicamente entre todos los usuarios.

Los procedimientos que manejan el transponder son asíncronos, por lo que no existe un control de la transferencia de datos desde el lector. Este es el caso, por ejemplo, del procedimiento *ALOHA*, el cual explicaremos con más detalle a continuación.

Estos procedimientos que controlan la etiqueta son, naturalmente, muy lentos e inflexibles. La mayoría de aplicaciones usan procesos que son controlados por el lector, tomando éste el papel de 'master'. Estos métodos pueden ser considerados como síncronos, ya que todos los tags son controlados y comprobados por el lector simultáneamente.

Un único transponder es primero seleccionado de un gran grupo de transponders en la zona de interrogación del lector usando un algoritmo concreto y entonces la comunicación tiene lugar entre la etiqueta seleccionada y el lector. Una vez acaba la comunicación, ésta se da por finalizada y entonces el lector selecciona otro tag. Sólo una única comunicación puede ser iniciada a la vez, pero los transponder trabajan en una rápida sucesión y parece que todo ocurre en el mismo instante de tiempo. Esta es la finalidad de los métodos TDMA.

Los procedimientos controlados por el lector se pueden subdividir en *'polling'* y *búsqueda binaria*. Todos estos métodos están basados en el principio de que todos los transponders son identificados por un único '*número de serie'*.

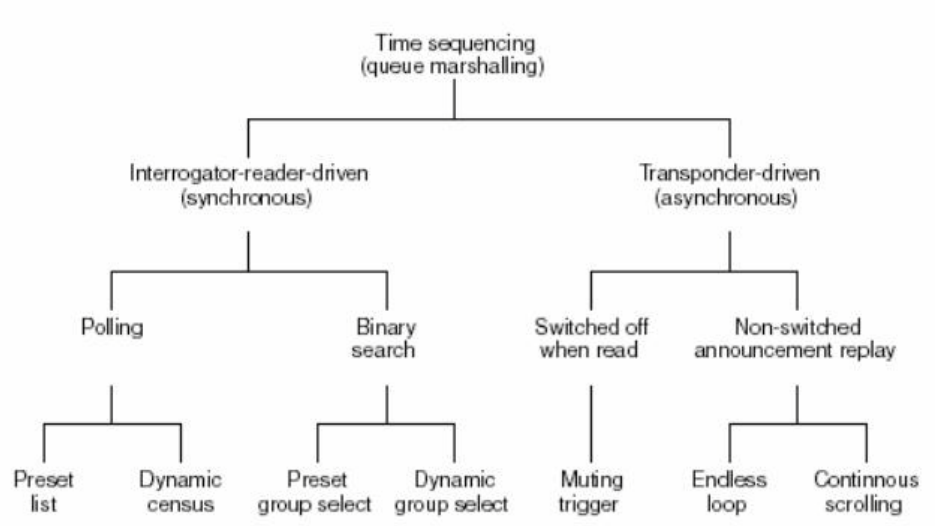


Figura 6.21 Clasificación de los métodos anticolisión TDMA según Hawkes (1997).

El método de '*polling'* requiere una lista de todos los 'números de serie' de las etiquetas que pueden encontrarse en todo momento dentro del área de lectura en una aplicación. Todos los códigos de los tags son interrogados por el lector uno a uno hasta que uno de los tags preguntados responde. Este proceso puede ser muy lento dependiendo del posible número de tags que pueda haber en la aplicación; por este motivo este método sólo es aplicable a sistemas que tengan un número pequeño de individuos a identificar.

El método de la *búsqueda binaria* es mucho más flexible además de ser uno de los procedimientos más comunes. Consiste en que el lector provoca, intencionadamente, una colisión con una etiqueta cualquiera, elegida al azar. Si el proceso tiene éxito, es imprescindible que el lector sea capaz de detectar en que precisa posición de todos los bits se ha producido la colisión usando un sistema de codificación conveniente. Una descripción comprensiva del método de la búsqueda binaria es explicado más adelante.

6.6.4 Métodos anticolisión más comunes

En los siguientes apartados vamos a explicar algunos de los métodos anticolisión más comúnmente usados. Los algoritmos de los ejemplos están intencionadamente simplificados de tal modo que el principio de funcionamiento puede ser entendido sin innecesarias complicaciones.

6.6.4.1 Método ALOHA

ALOHA es el más simple de todos los métodos anticolisión. Su nombre proviene del hecho de que este método multiacceso fue desarrollado en los años 70 por ALOHANET – una red de radiocomunicaciones de datos de Hawai.

Este proceso es usado exclusivamente con transponders de sólo-lectura, los cuales generalmente tienen que transmitir sólo una pequeña cantidad de datos (número de serie o código), estos datos que son enviados al lector son una secuencia cíclica.

El tiempo de transmisión de los datos es tan sólo una fracción del tiempo de repetición, ya que hay pausas relativamente largas entre las transmisiones. Sin embargo, los tiempos de repetición para cada etiqueta difieren levemente. Existe una elevada probabilidad de que dos transponders puedan transmitir sus paquetes de datos en tiempos diferentes y, así, de que no colisionen el uno con el otro.

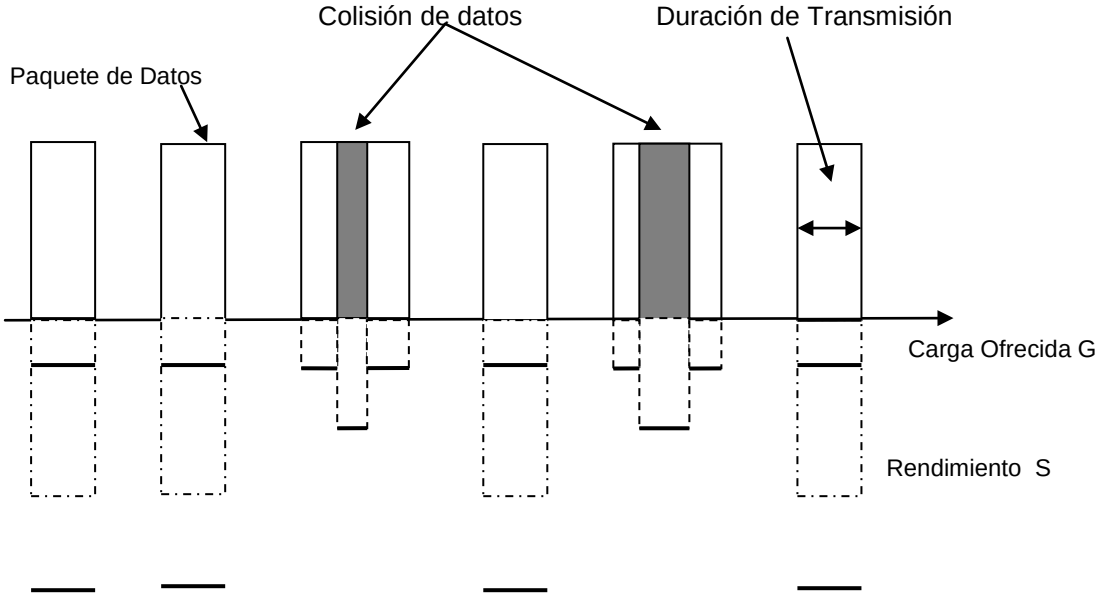


Figura 6.22 Secuencia temporal de una transmisión en un sistema ALHOA.

El tráfico ofrecido G corresponde al número de etiquetas transmitiendo simultáneamente en un cierto punto temporal tn. El tráfico medio ofrecido G es la media de la observación en un periodo de tiempo T y es extraordinariamente sencillo de calcular a partir de tiempo de transmisión de un paquete de datos:

$$G = \sum_{1}^{n} \frac{\tau_n}{T} \cdot r_n \qquad (6.1)$$

donde n=1, 2,3,... corresponde al número de tags en un sistema y rn=0, 1,2,… es el número de paquetes de datos que son transmitidos por el transponder *n* durante el periodo de observación. El throughput *s* es 1 por la duración de la transmisión libre de errores (sin colisión) de un paquete de datos. En todos los casos en los que no haya una transmisión sin colisión (no existe transmisión o no se puede leer el paquete de datos por culpa de un error provocado por una colisión) el valor del throughput es 0. El throughput medio *S* de un canal de transmisión es hallado a partir del tráfico ofrecido G:

$$S = G \cdot e^{(-2G)} \tag{6.2}$$

Si consideramos el throughput *S* en relación con el tráfico ofrecido G (ver ecuación 6.2) encontramos un máximo de un 18'4% para una G=0,5. Para tráfico ofrecido menor, el canal de transmisión permanecerá sin usar la mayoría del tiempo; si el tráfico ofrecido se incrementa por el número de colisiones entre cada una de las etiquetas entonces *S* se incrementaría agudamente.

La probabilidad de éxito *q* – la probabilidad de que un único paquete pueda ser transmitido sin colisiones – puede ser calculada a partir del tráfico medio ofrecido G y el throughput *S*:

$$q = \frac{S}{G} = e^{(-2G)} \tag{6.3}$$

Gracias a esta ecuación, algunos datasheets (hojas de especificaciones) incluyen figuras donde se muestra el tiempo necesario para ser capaz de leer todos los transponders que se encuentran en la zona de interrogación – lo que depende, evidentemente, del número de transponders que se encuentren dentro de la zona de interrogación.

La probabilidad *p (k)* de que una transmisión observada en un periodo T tenga *k* paquetes libres de errores puede ser calculada a partir del tiempo de transmisión τ de un paquete de datos y del tráfico medio ofrecido G. La probabilidad *p (k)* es una distribución de Poisson con valor medio G/τ:

$$p(k) = \frac{\left(G \cdot \frac{T}{\tau}\right)^k}{k!} \cdot e^{\left(-G\frac{T}{\tau}\right)} \tag{6.4}$$

6.6.4.2 Método ALOHA Ranurado

Una posibilidad para mejorar el relativamente bajo throughtput del método ALOHA es el método ALOHA Ranurado, mediante el cual las etiquetas sólo empiezan a transmitir en unos instantes de tiempo definidos y síncronos (*time slots).* La necesaria sincronización de las etiquetas es realizada por el lector.

El periodo de tiempo en el cual una colisión puede ocurrir (intervalo de colisión) es la mitad del mejor de los casos que se pueden dar en el método ALHOA.

Si asumimos que los paquetes de datos tienen todos igual tamaño (y por lo tanto tienen el mismo tiempo de transmisión T) una colisión puede ocurrir en el método ALOHA si dos transponders quieren transmitir un paquete de datos hacia el lector en un intervalo de tiempo $2T$. Como en ALOHA ranurado sólo pueden transmitirse paquetes en determinados puntos temporales, el intervalo donde se puede tener una colisión queda reducido a T. Esto provoca la siguiente relación para el throughput del método ALOHA ranurado:

$$S = G \cdot e^{(-G)} \tag{6.5}$$

Como vemos en la Figura 6.23, si usamos el método ALOHA ranurado podemos llegar a tener un throughput máximo *S* de 36,8% para un tráfico ofrecido G.

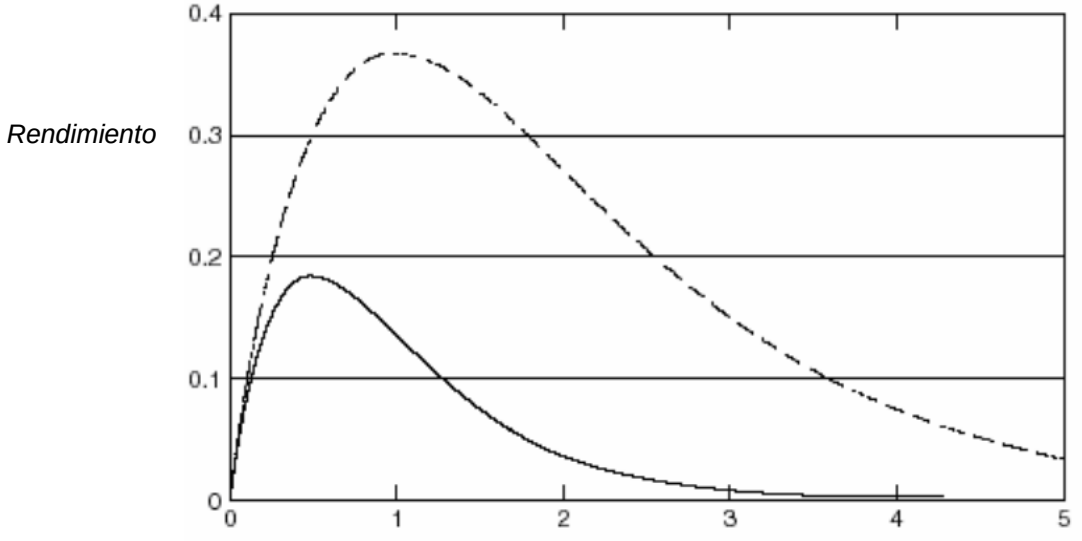


Figura 6.23 Comparación de las curvas del throughput de ALOHA y ALOHA ranurado. En ambos métodos el throughput tiende a cero tan pronto como el punto máximo ha sido sobrepasado

De todos modos no es necesario que, si varios transponder envían su información al mismo tiempo, exista colisión: si una etiqueta está más cerca del lector que las demás puede ser capaz de imponerse a las demás como resultado de una mejor intensidad de su señal en el lector (debido a la proximidad de ésta al lector). Esto es conocido como el *efecto captura*.

El efecto captura tiene un efecto muy beneficioso en el comportamiento del throughput. Decisivo para esto es el '*threshold' b* el cual indica como de 'fuerte' es un paquete de datos enviados respecto a los otros para ser detectado por el receptor sin errores.

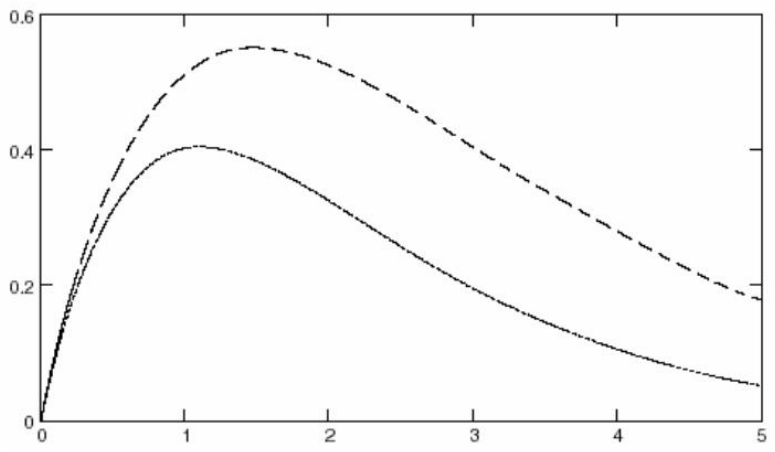
$$S = G \cdot e^{\left(\frac{b \cdot G}{1+b}\right)} \tag{6.6}$$

Los principales comandos usados para controlar el proceso de anticolisión son:

REQUEST	*Este comando sincroniza todos los transponders en el área de lectura y les solicita que transmitan sus números de serie al lector en uno de los time slots que haya a continuación.*
SELECT (SNR)	*Envía, como parámetro, un número de serie previamente seleccionado (SNR) al transponder. El transponder que tiene este número se prepara para poder recibir comandos de lectura o escritura. Los transponders con diferente número de serie siguen con el comando REQUEST como acción principal*
READ_DATA	*El transponder seleccionado envía los datos almacenados al lector (existen sistemas que también tienen comandos de escritura, autenticación, etc.)*

Tabla 6.5 Comandos para proceso de anticolisión

Throughput



Carga Ofrecida G

——— *3 dB*
- - - - - - - *10 dB*

Figura 6.24 Comportamiento del throughput teniendo en cuenta el efecto captura con thresholds de 3 y 10 dB.

En el siguiente gráfico vemos un ejemplo del comportamiento de un sistema con el método ALHOA ranurado:

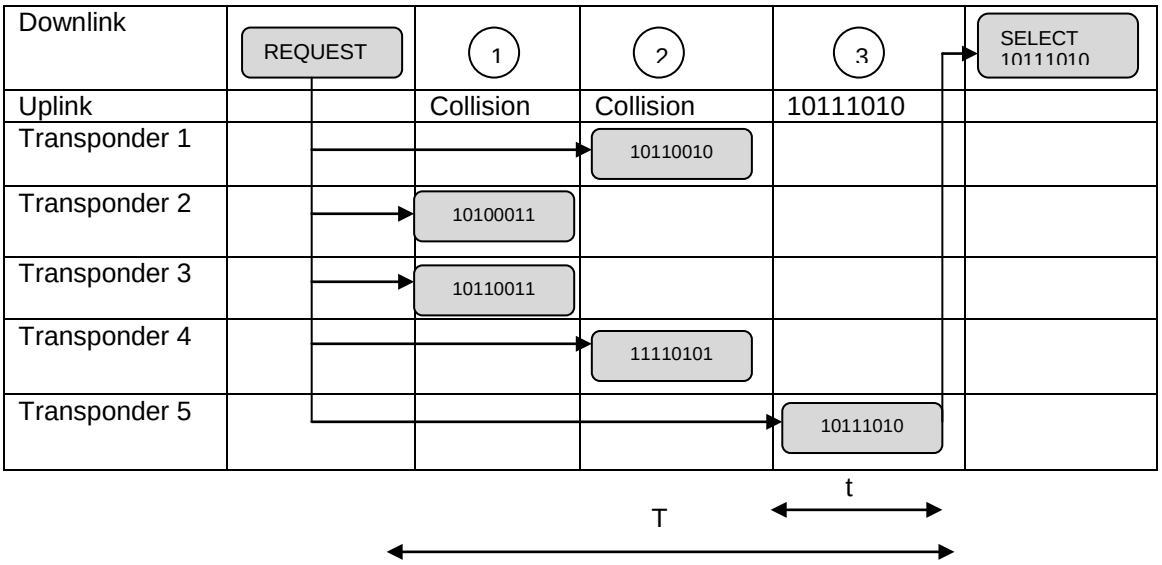


Figura 6.25 Ejemplo de sistema con el método anticolisión ALHORA ranurado

En el ejemplo que tenemos, los transponders tienen códigos de 8 bits, lo que limita a 256 los posibles tags puede haber en el sistema. En el momento en que el lector realiza el "REQUEST", cada uno de los cinco transponders que se encuentran en el área de interrogación elige un slot temporal de los tres posibles que hay. De este modo vemos como se produce la colisión de dos transponders en los dos primeros slots temporales, mientras que el tag que ha elegido el tercer slot llega al lector, realizando ya el siguiente proceso de "SELECT".

Este método seguirá hasta que el lector haya realizado las operaciones que pretende realizar y entonces seguirá con los demás tags.

6.6.5 Algoritmo de búsqueda binaria

La implementación del algoritmo de la búsqueda binaria requiere que el bit preciso donde se produce la colisión sea localizado por el lector. Además, se necesita del uso de una codificación de bit conveniente; por eso vamos primero a comparar el comportamiento en las colisiones de las codificaciones NRZ y Manchester.

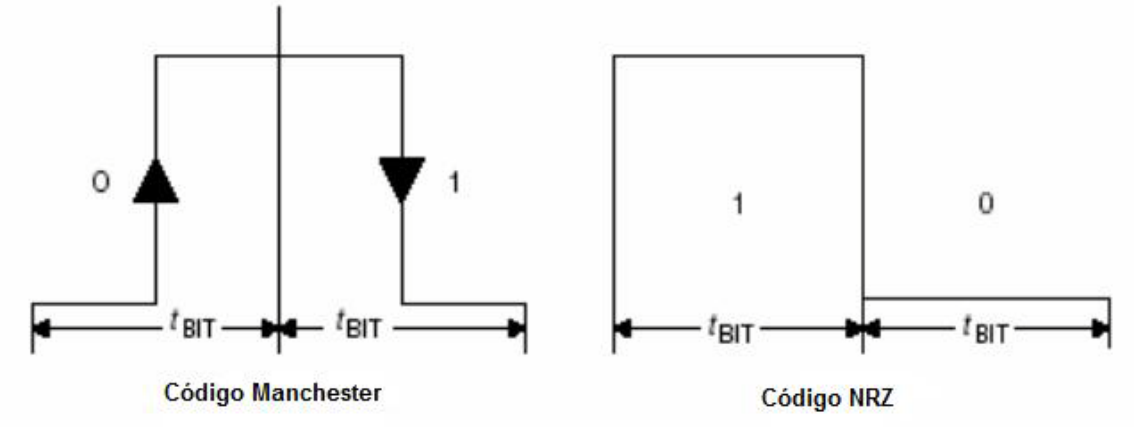


Figura 6.26 Codificación de bit usando códigos Manchester y NRZ

Usando el Código NRZ ante una colisión

El valor de un bit es definido por el nivel estático del canal de transmisión durante una 'ventana de bit' (*tBIT)*. En nuestro ejemplo anterior un '1' lógico es codificado por un nivel 'alto' estático, mientras que un '0' lógico lo es por un nivel 'bajo' estático.

Si al menos uno de los dos transponders envía una subportadora, esta es interpretada por el lector como una señal 'alta' y, en nuestro ejemplo, es asignada al valor lógico '1'. El lector no puede detectar si la señal que está recibiendo es una señal proveniente de la superposición de las señales de dos transponders o si, por el contrario, es una señal proveniente de un único tag y, por lo tanto, válida. El uso de un bloque de control de errores (paridad, CRC, etc.) puede encontrar el error en cualquier parte de un bloque de datos. De hecho no lo localiza, simplemente detecta la existencia de un error.

Usando el Código Manchester ante una colisión

El valor de un bit es definido por el cambio de nivel (transición positiva o negativa) durante una ventana de bit (*tBIT*). En el ejemplo anterior un '0' lógico es codificado por una transición positiva; un '1' lógico es codificado por una transición negativa. El estado de 'no transmisión' no está permitido durante la transmisión de datos y es reconocido como un error.
Si dos (o más) transponders transmiten simultáneamente bits de diferente valor, entonces unos cancelan a los otros y lo que sucede que es que el lector recibe un valor constante de señal durante todo el periodo de bit, lo que es reconocido como un error ya que este es un estado no permitido por la codificación Manchester. Así es posible detectar la colisión de un bit concreto.

Usaremos el código Manchester en nuestro ejemplo para explicar el algoritmo de búsqueda binaria

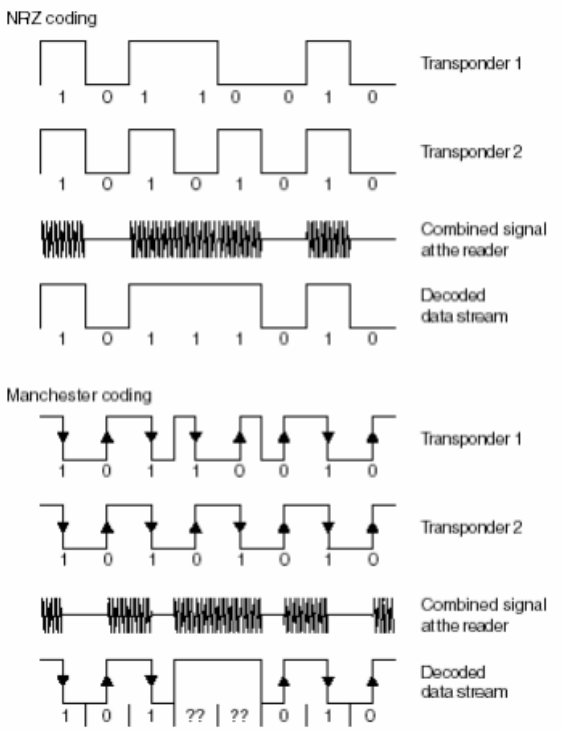


Figura 6.27 Comportamiento de los códigos Manchester y NRZ ante una colisión. El código Manchester hace posible detectar la colisión de un bit concreto.

Un algoritmo de búsqueda consiste en una secuencia predefinida (especificación) de interacciones (comando y respuesta) ente el lector y el transponder con el objetivo de ser capaz de seleccionar un transponder concreto de todos los pertenecientes a un grupo grande.

Para la realización práctica del algoritmo requerimos un conjunto de comandos que puedan ser procesados por el transponder. Además cada transponder debe tener un único número de serie (por ejemplo un código EPC). En el ejemplo que explicamos a continuación usamos un número de serie de 8 bits, por lo que tan sólo podemos garantizar 28 códigos distintos (256 códigos) y, por lo tanto, tan sólo podrá haber 256 etiquetas en el sistema.

REQUEST	*Este comando manda un número de serie a los transponders como parámetro. Si el número de serie del transponder que lo recibe es menor o igual que el número de serie que manda el lector, entonces el transponder manda su propio número de serie hacia el lector. Así el grupo de transponders que responden pueden ser preseleccionados y reducidos.*
SELECT (SNR)	*Envía, como parámetro, un número de serie previamente seleccionado (SNR) al transponder. El transponder que tiene este número se prepara para poder recibir comandos de lectura o escritura. Los transponders con diferente número de serie tan sólo responderán a un REQUEST.*
READ_DATA	*El transponder seleccionado envia los datos almacenados al lector (existen sistemas que también tienen comandos de escritura, autenticación, etc.)*
UNSELECT	*La selección de un transponder preseleccionado anteriormente se cancela y el transponder es 'silenciado'. En este estado el tag está completamente inactivo y no responder a los REQUEST. Para reactivarlo, debe ser reseteado apartándolo temporalmente del área del interrogación del lector (lo que es lo mismo que cortarle la fuente de alimentación).*

Tabla 6.6 Comandos para algoritmo de búsqueda binaria

El uso de los comandos que acabamos de definir en el algoritmo de búsqueda binaria será demostrado basado en el funcionamiento de un ejemplo con cuatro etiquetas dentro del área de interrogación. Los transponders de nuestro ejemplo poseen un único número de serie dentro del rango 00 – FFh (= 0 – 255 dec. o 00000000 – 11111111 bin.).

Transponder 1	10110010
Transponder 2	10100011
Transponder 3	10110011
Transponder 4	11100011

Tabla 6.7 Lista de transponders usados.

La primera iteración del algoritmo empieza con la transmisión del comando REQUEST (≤11111111) por parte del lector. El número de serie 11111111b es el más grande posible, así que con este comando se preguntaría a todos los transponders dentro del área de interrogación.

La precisa sincronización de todas las etiquetas, por lo que empiezan a transmitir todas sus números de serie exactamente en el mismo instante de tiempo, es muy importante para conseguir un funcionamiento seguro del *árbol del algoritmo de búsqueda binaria*. Sólo de este modo es posible una precisa localización de bit donde se ha producido la colisión.

Como vemos en la tabla que viene a continuación, tenemos colisión (X) en los bits 0, 4 y 6 del número de serie recibido como superposición de las diferentes secuencias de los transponder que han respondido. El hecho de que haya una o más colisiones en los números de serie recibidos los lleva a pensar que tenemos más de un tag dentro del área de interrogación. Para ser más precisos, la secuencia de bits recibida 1X1X001X nos indica que tenemos aún ocho posibilidades de números de serie que tienen que ser detectados.

Número de Bit	7	6	5	4	321	0
Datos recibidos en el lector	1	X	1	X	001	X
Posible número de serie A	1	0	1	0	001	0
Posible número de serie B*	1	0	1	0	001	1
Posible número de serie C*	1	0	1	1	001	0
Posible número de serie D*	1	0	1	1	001	1
Posible número de serie E	1	1	1	0	001	0
Posible número de serie F*	1	1	1	0	001	1
Posible número de serie G	1	1	1	1	001	0
Posible número de serie H	1	1	1	1	001	1

Tabla 6.8 Posibles números de serie después de evaluar los datos recibidos y y teniendo en cuenta las colisiones (X) que han ocurrido en la primera iteración. Cuatro de las posibles direcciones (*) son las toman fuerza aquí.

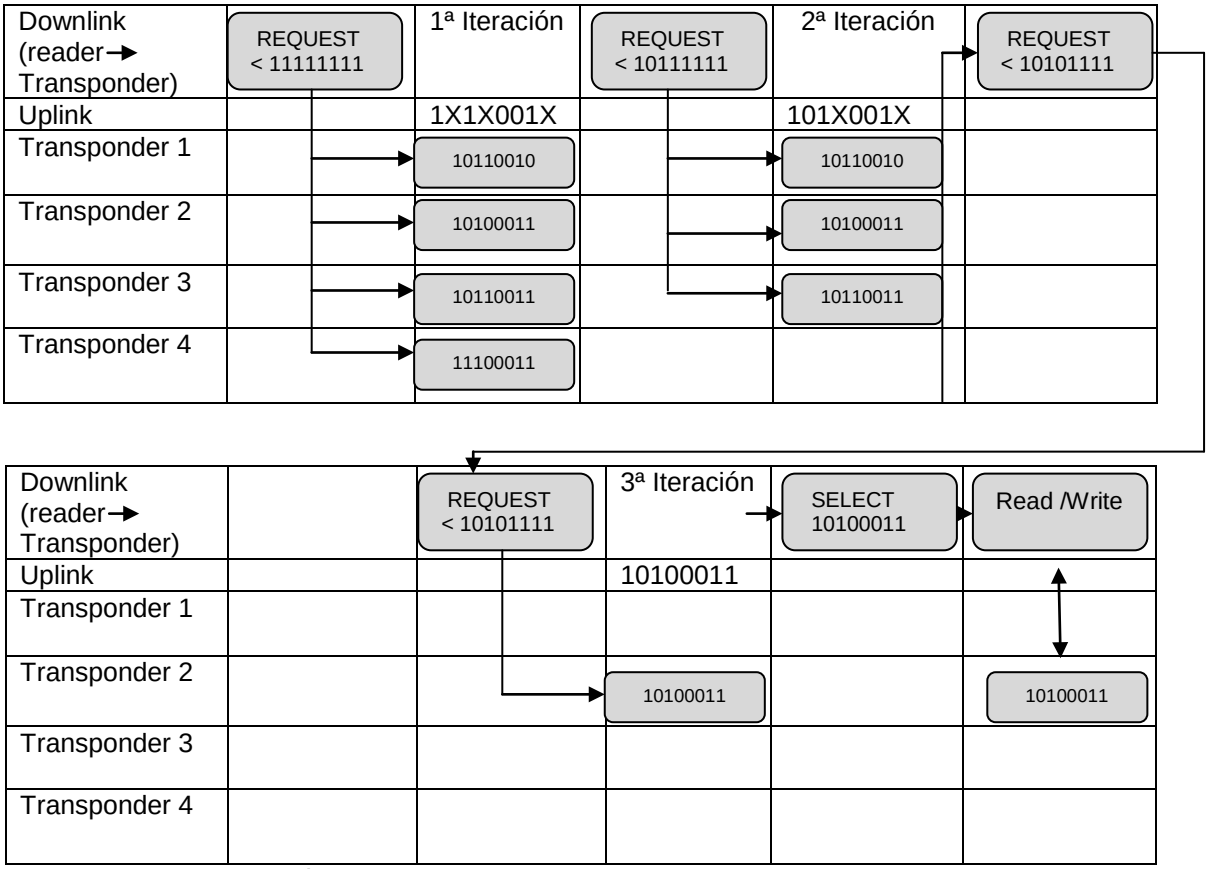


Figura 6.28 Los diferentes números de serie que son devueltos por los transponder en respuesta al comando REQUEST provocan una colisión. Por la restricción selectiva del rango preseleccionado de direcciones en las siguientes iteraciones, finalmente un solo tag responderá.

Comando de Búsqueda	**Rango Primera Iteración**	**Rango Iteración n =**
REQUEST >=	0	(Bit X) = 1, Bit (0 To X – 1) = 0
REQUEST<=	SNRmax	(Bit X) = 0, Bit (0 To X – 1) = 1

Tabla 6.9 Regla general para formar el parámetro dirección en el árbol de la búsqueda binaria. En cada caso, el bit (X) es el de mayor peso de la dirección recibida desde el transponder en el cual ha ocurrido una colisión en la iteración inmediatamente anterior.

Después de que el lector haya transmitido el comando REQUEST (≤11111111), todos los transponders que cumplen esta condición responderán enviando su número de serie al lector. En nuestro ejemplo estos son los transponders 1, 2 y 3.

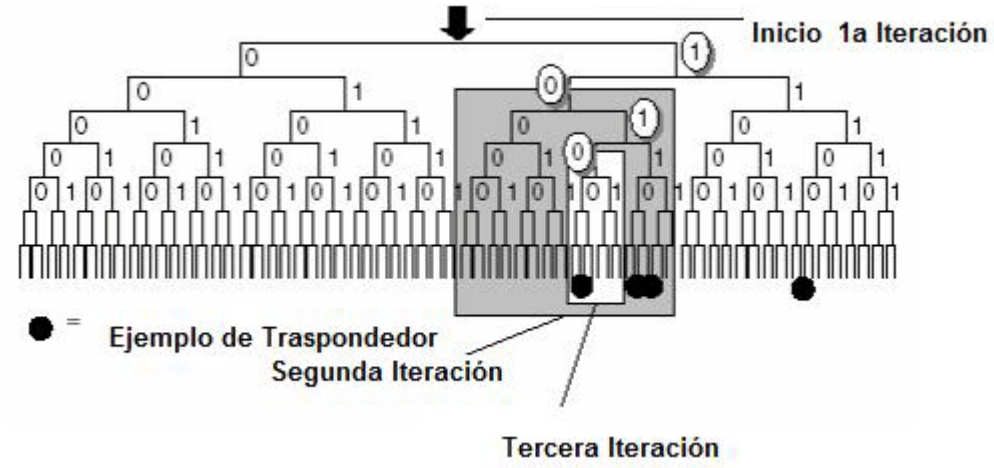


Figura 6.29 Árbol de búsqueda binaria. Un único transponder puede ser seleccionado por sucesivas reducciones del rango de etiquetas posibles.

Ahora hay una colisión (X) de los bits 0 y 4 del número de serie recibido. A partir de esto podemos sacar la conclusión de que hay, al menos, dos transponders en el rango de la segunda iteración. La secuencia recibida 101X001X aún permite 4 opciones para los posibles números de serie a detectar.

Número de Bit	765	4	321	0
Datos recibidos del lector	101	X	001	X
Posible número de serie A	101	0	001	0
Posible número de serie B*	101	0	001	1
Posible número de serie C*	101	1	001	0
Posible número de serie D*	101	1	001	1

Tabla 6.10 Posibles números de serie en el rango de búsqueda después de evaluar la segunda iteración. Los transponders marcados (*) son los más probables actualmente.

La nueva aparición de colisiones en la segunda iteración requiere una nueva restricción del rango de búsqueda en una tercera iteración. El uso de la regla de la tabla (2.14) nos lleva al rango de búsqueda ≤10101111. Ahora el lector vuelve a transmitir a las etiquetas el comando REQUEST (≤10101111). Esta condición es, finalmente, cumplida sólo por el transponder 2, el cual responde ahora al comando sin que exista colisión posible. Así hemos detectado un número de serie válido – ya no es necesaria una nueva iteración.

Gracias al siguiente comando que hemos explicado (SELECT), el transponder 2 es seleccionado usando la dirección detectada y puede ser ahora leído o escrito sin interferencias por parte de los

otros transponders. Todos los tags están 'callados' y sólo el seleccionado responde al comando de lectura/escritura – READ_DATA.

Después de completar la operación de lectura/escritura, el transponder 2 puede ser completamente desactivado usando el comando UNSELECT, de manera que no responda al próximo comando REQUEST. De este modo el número de iteraciones necesario para seleccionar los demás transponders irá disminuyendo gradualmente.

La media de iteraciones L necesaria para detectar un único transponder de entre un gran número de ellos depende del número total de transponders *N* que se encuentran en el área de interrogación del lector, y puede ser calculada fácilmente:

$$L(N) = ld(N) + 1 = \frac{\log(N)}{\log(2)} + 1 \qquad (6.7)$$

Si tan sólo un transponder se encuentra en la zona de interrogación del lector, entonces tan sólo se requiere una iteración para detectar su número de serie – no existe colisión en este caso. Si hay más de un transponder en la zona de interrogación del lector, entonces el número medio de iteraciones va incrementando gradualmente, siguiendo la curva

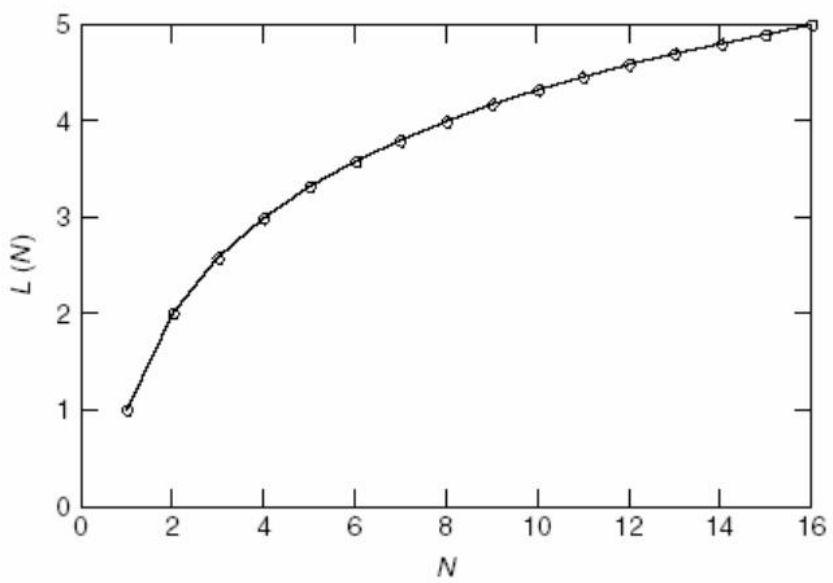
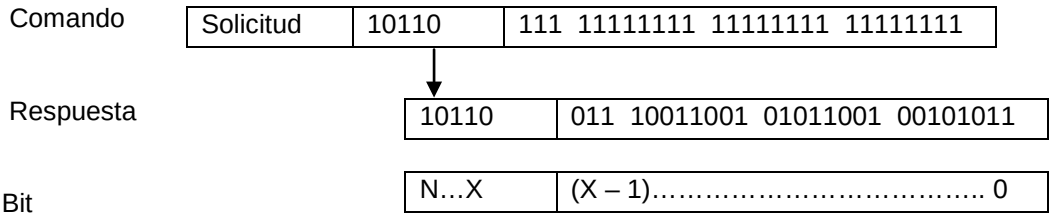


Figura 6.30 El número medio de iteraciones necesitado para determinar la dirección del transponder (número de serie) de un único transponder en función del número total de transponders que se encuentran en el área de interrogación. Cuando tenemos 32 transponders en el área de interrogación hacen falta una media de seis iteraciones, para 65 transponders una media de siete, para 128 transponders una media de ocho iteraciones, etc.

6.6.6 Algoritmo de la búsqueda binaria dinámica

En el método de la búsqueda binaria que vamos a explicar, el criterio de búsqueda y el número de serie de los transponders son siempre transmitidos en su longitud total. En la práctica, de todos

modos, los números de serie de los transponders no consisten en un solo byte, como en el ejemplo, sino que dependiendo del sistema puede tener más de 10 bytes, lo que significa que toda esta información debe ser transmitida para poder seleccionar un único transponder. Si investigamos el flujo de datos entre el lector y los transponders individualmente y en más detalle encontramos que:



- Desde el bit (X-1) al 0 del comando REQUEST no contiene información adicional a partir del momento en que se fijan todos los bits a 1.
- Desde el bit N al X del número de serie en la respuesta del transponder no contiene información adicional para el lector ya que es una información predeterminada y, por lo tanto, conocida.

Por lo tanto vemos que las partes complementarias de la información adicional transmitida son redundantes y que, por eso mismo, no necesitan ser transmitidas. Esto nos muestra rápidamente que podemos encontrar un algoritmo optimizado. En vez de transmitir toda la longitud de los números de serie en ambas direcciones, se puede partir teniendo en cuenta el bit X. El lector ahora tan sólo manda la parte conocida (N - X) del número de serie para ser determinado como el criterio de búsqueda en el comando REQUEST y entonces interrumpe la transmisión. Todos los transponders que coinciden en sus bits N al X con el criterio de búsqueda, responden enviando los bits que faltan, es decir, del X-1 al 0 de su número de serie. Los transponders son informados del número de bits de la subsecuencia por un parámetro adicional (*NVB=número válido de bits)* en el comando REQUEST.

Si nos fijamos en el ejemplo que hemos descrito en el apartado de *Algoritmo de búsqueda binaria* y lo aplicamos ahora, vemos que desde que aplicamos la regla de la tabla (2.14) el número de iteraciones corresponde con las del ejemplo anterior pero, sin embargo, el número de bits transmitidos - y por lo tanto el número de tiempo necesitado – puede ser reducido por debajo del 50%.

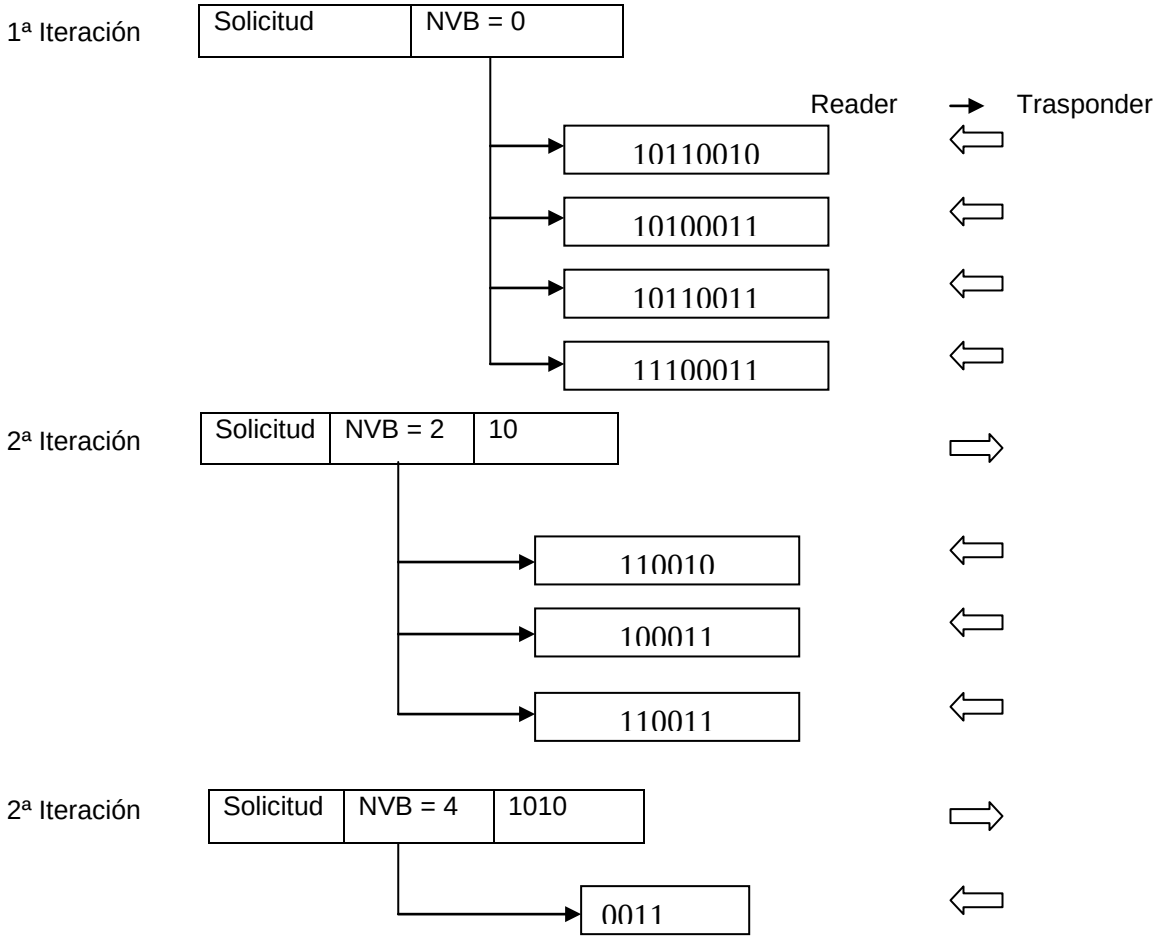


Figura 6.31 El algoritmo de búsqueda binaria dinámico evita la transmisión de partes redundantes del número de serie. El tiempo de transmisión es, así, reducido considerablemente.

7. Regulación y Estandarización

La RFID está concentrando alrededor suyo cada vez más atención, y cada vez más en los términos correctos: aumenta la disponibilidad de información, se multiplican los análisis de beneficios que podemos esperar de su utilización en cualquier medio profesional, se valoran las posibilidades técnicas relacionadas con cada una de sus muchas versiones. Y al mismo tiempo, también la normativa internacional relativa a dichas tecnologías está por definirse completamente, un requisito básico para su difusión real en el mundo y su utilización como instrumento de identificación. En el presente capitulo con, se ofrece una panorama, que completo, acerca de los estándares internacionales tanto de naturaleza técnica como de aplicación.

7.1 Consideraciones previas

Si durante su primera fase de desarrollo, podían aceptarse soluciones técnicas que se definían propietarias, las aplicaciones multi-usuario que se vislumbran hoy precisan por el contrario de soluciones normalizadas, las únicas que pueden permitir la interoperabilidad de los diferentes sistemas propuestos por los proveedores de soluciones y, por ello, que puedan utilizar todos los usuarios en cualquier parte del mundo.

Considerando la globalización de la economía, dicha interoperabilidad es una necesidad absoluta. Y, además, en cuanto se publiquen todos los estándares o normas internacionales, también los que utilizan sistemas en medios cerrados podrán beneficiarse de la misma interoperabilidad, para poner en marcha oportunas dinámicas de competencia. La puesta en juego de dichas normas es, por lo tanto, mundial y coloca la labor de normalización en el centro del debate actual acerca del futuro de la RFID. Todas las investigaciones demuestran que la falta de normas ha sido, y sigue siendo, uno de los motivos de incertidumbre para los usuarios potenciales. Sin embargo, gracias a la significativa labor de todos los agentes implicados en la labor de normalización, ante todo la ISO (International Standard Organisation), hoy se pueden tener sistemas realmente interoperables.

7.2 Regulación

En lo que respecta al uso de frecuencias, dependiendo de la banda en la que queramos trabajar, se debe tener en cuenta que según donde nos encontremos tendremos que guiarnos por las recomendaciones que tenemos a continuación.

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 Khz. y 140 - 148.5 Khz.) y de alta frecuencia (HF: 13.56 MHz) se pueden utilizar de forma global sin necesidad de licencia ya que trabajan

dentro de la banda ISM (Industrial – Scientific – Medical). La frecuencia UHF (868 - 928 MHz) no puede ser utilizada de forma global, ya que no hay un único estándar global. En Estado Unidos, la frecuencia UHF se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la potencia de transmisión. En Europa la frecuencia UHF está permitida para rangos entre 865.6 - 867.6 MHz y en México de 450.2 – 468.9 MHz. Sin embargo existen diferentes restricciones en la potencia de transmisión para cada uno de los diferentes países así como la prohibición del uso de estas frecuencias en zonas fronterizas.

El estándar UHF norteamericano (908-928 MHz) no es aceptado en Francia ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de las frecuencias UHF. Cada aplicación de frecuencia UHF en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales, y puede ser revocada. En Australia y Nueva Zelanda, el rango es de 918 - 926 MHz para uso sin licencia, pero hay restricciones en la potencia de transmisión.
Existen regulaciones adicionales relacionadas con la salud y condiciones ambientales. Por ejemplo, en Europa, la regulación *Waste of electrical and electronic equipment* ("Equipos eléctricos y electrónicos inútiles"), no permite que se desechen las etiquetas RFID. Esto significa que las etiquetas RFID que estén en cajas de cartón deber de ser quitadas antes de deshacerse de ellas.
También hay regulaciones adicionales relativas a la salud; en el caso de Europa acaba de publicarse (por parte de la ETSI) un estándar llamado EN 302 208 que consta de dos partes.
Las especificaciones que cumple son:

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (R&TTE Directive).
CEPT/ERC/REC 70-03: "Relating to the use of Short Range Devices (SRD)".
ETSI EN 301 489-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements".
ETSI TR 100 028 (all parts): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Uncertainties in the measurement of mobile radio equipment characteristics".
ETSI EN 302 208-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W Part 1: Technical requirements and methods of measurement".
ETSI EN 301 489-3: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz".
Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits (LV Directive).
Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive).

Tabla 7.1 Especificaciones que cumple la norma EN 302 208

7.2.1 Organizaciones de regulación y normalización

No existe una verdadera entidad de normalización internacional, al depender la atribución y la regulación de las frecuencias a la soberanía nacional. Es, por lo tanto, siempre necesario, para cada usuario, comprobar que los productos que está utilizando respeten las leyes vigentes en cada país. Para simplificar, podría afirmarse que las entidades de regulación establecen la frecuencia o la banda de frecuencia (como en el caso de la UHF), la potencia de emisión y el tiempo máximo de comunicación entre etiquetas y lectores [30].

Por tales motivos cada país regula a su conveniencia la tecnología RFID. Y en lo que respecta a la estandarización es la ISO quien define los estándares comerciales e industriales a nivel mundial, y la IEC8 promueve la cooperación internacional para la estandarización en los campos de la electrónica y las tecnologías. Ambos organismos definen los estándares ISO/IEC.

Sin embargo no existe ninguna administración que se encargue de la regulación a nivel global de la tecnología RFID, sino como se menciono anteriormente cada país tiene sus órganos propios mediante los cuales regula de un modo individual el uso que se hace de las frecuencias y las potencias permitidas dentro de su propio territorio. Algunos de los organismos internacionales que regulan la asignación de frecuencias y potencias para RFID son:

- **EE.UU**.: FCC (*Federal Communications Commission*)
- **Canadá**: DOC (*Departamento de la Comunicación*)
- **México**: COFETEL (Comisión Federal de Telecomunicaciones)
- **Europa**: CEPT (siglas de su nombre en francés *Conférence européenne des administrations des postes et des télécommunications)*, ETSI (*European Telecommunications Standards Institute*, creado por el CEPT) y administraciones nacionales. Obsérvese que las administraciones nacionales tienen que ratificar el uso de una frecuencia específica antes de que pueda ser utilizada en ese país
- **Japón**: MPHPT (*Ministry of Public Management, Home Affairs, Post and Telecommunication*)
- **China**: Ministerio de la Industria de Información
- **Australia**: Autoridad Australiana de la Comunicación (*Australian Communication Authority*)
- **Nueva Zelanda**: Ministerio de desarrollo económico de Nueva Zelanda (*New Zealand Ministry of Economic Development*)

En el caso de México es la COFETEL la encargada de regular todo lo relacionado al uso de las radio frecuencias sin importar el fin que tengan los sistemas en este caso sistemas RFID si es que estuviera tipificado en la ley.

Sin embargo en nuestro país aun no se ha legislado en materia de la RFID como lo han hecho países como Estados Unidos, Cánada, Japón, Inglaterra y en todos los países pertenecientes a la Unión Europea sin embargo se han presentado iniciativas de ley para legislar en lo que concierte a la implantación de "chips-antisecuestros" en el cuerpo humano los cuales trabajan con RFID y localización GPS debido a que algunas de las compañías que prestan este servicio abandonan a la persona que se le implanto uno de estos chips cuando esta por algunos motivos deja de pagar la cuota, con el chip dentro su cuerpo.

Sin embargo fuera de estos casos aun no se han presentado iniciativas de ley para la regulación de la tecnología RFID.

7.3 Estándares ISO

Para comprender correctamente cómo están estructuradas todas las normas publicadas, ante todo hay que distinguir las normas "técnicas" de las "de aplicación". Normas "técnicas", significa toda las normas que atañen a la comunicación entre el lector y las etiquetas, así como la gestión de los datos contenidos en dichas etiquetas.

Así mismo, las normas "de aplicación" son normas establecidas según la categoría de usuario, que puede utilizar o no utilizar dichas normas técnicas.

Para mayor precisión también cabe distinguir las normas que atañen a la trazabilidad de las personas y las transacciones financieras, que prevén la utilización de tarjetas inteligentes sin contacto, de las normas que atañen a la trazabilidad de los objetos.

7.3.1 Entidades de normalización ISO

Cabe destacar que en lo que se refiere a las normas técnicas, la entidad de normalización no es el ISO, sino un Joint Technical Committee (JTC) compuesto a partir del ISO y el IEC, llamado ISO/IEC/JTC1. En dicho JTC, dos subcomités se reparten la tarea: el subcomité 17 aborda los primeros (trazabilidad de las personas) y el subcomité 31 aborda los segundos (trazabilidad de los objetos). En lo que se refiere a la trazabilidad de los objetos mediante RFID, el subcomité 31 ha repartido la tarea entre cuatro grupos de trabajo (Working Groups):

- WG2: Work Group on Data Structure
- WG3: Work Group on Conformance
- WG4: Work Group on RFID Item Management

- Finalmente el WG5, creado hace poco, a finales de 2004, se ocupa de geolocalización en tiempo real, o Real Time Locating System (RTLS).

7.3.1.1 Trazabilidad de las personas

La trazabilidad de las personas, como se ha dicho, la lleva a nivel internacional el subcomité ISO/IEC/JTC1/SC17, y en Francia, a nivel CN17 del AFNOR. Son dos las normas vigentes desde hace algunos años, producidas por el ISO/IEC/SC17/WG8 sobre tarjetas inteligentes sin contacto: la 14443 para lecturas a pocos milímetros ("vecindad") y la 15693 para lecturas a unos cuantos centímetros ("proximidad") [31].
Ambas utilizan la frecuencia 13,56 MHz y las etiquetas tienen el formato estándar de las tarjetas inteligentes.

7.3.1.2 Trazabilidad de los objetos

La trazabilidad de las personas la lleva a nivel internacional el subcomité ISO/IEC/JTC1/SC31 (JTC1/SC31/WG3 - pruebas; JTC1/SC31/WG4 - protocolos; JTC1/SC31/WG5 - RTLS).
Presentadas como la solución por excelencia a los problemas de interoperabilidad, las normas 18000 no son en realidad suficientes, de por sí solas, para lograr dicho objetivo, se precisa de dos condiciones: por un lado, la utilización de un protocolo común para la comunicación entre el lector y la etiqueta, que es efectivamente la materia de las normas 18000, y por otro, la organización única de las estructura de datos contenidos en el chip. Las normas 18000 forman parte de un grupo de normas que ya se han publicado y que, tomadas en su conjunto, permiten lograr la interoperabilidad [32].

7.3.2 ISO/IEC 18000

SO/IEC 18000 Information Technology - Automatic Identification and Data Capture Techniques - RFID for item Management - Air Interface.

Proporcionan los valores concretos para la definición de la interfaz de aire para los parámetros de una particular frecuencia y tipo de interfaz de aire a partir de la cual se puede establecer el cumplimiento o incumplimiento con la parte 1 de la norma ISO / IEC 18000

Estan integradas por:

ISO/IEC 18000-1 - Generic Parameters for Air Interface - Communication for Globally Accepted Frequencies

ISO/IEC 18000-2 - Parameters for Air Interface Communications below 135 KHz

Nota: Se utilizan dos tipos de productos: el tipo A, llamado "Full Duplex" o FDX en 125 KHz, y el tipo B llamado "Half Duplex" o HDX en 134,2 KHz. Ambos difieren por la capa física, sin embargo utilizan el mismo protocolo.

ISO/IEC 18000-3 - Parameters for Air Interface Communications at 13,56 MHz

Nota: se utilizan 2 modos. El modo 1 derivado de la norma 15693 para las tarjetas sin contacto, y el modo 2 derivado de la tecnología desarrollada por la compañía Magellan (Australia) y cuya característica es la de permitir una velocidad de intercambio de datos mucho más rápida (hasta 40 veces). Nota: estos dos modos no son interoperables entre sí.

ISO/IEC 18000-4 - Parameters for Air Interface Communications at 2,45 GHz

Nota: También en este caso son dos los modos utilizados, y corresponden a dos sistemas desarrollados por las compañías Intermec® y Siemens/Nedap®

ISO/IEC 18000-6 - Parameters for Air Interface Communications at UHF (from 860 to 960 MHz)

Nota: Son tres los tipos utilizados. El tipo A utiliza el sistema "Pulse Interval Encoding (PIE) with slotted ALOHA collision arbitration protocol"; el tipo B utiliza el sistema "Manchester Encoding with Binary Tree collision arbitration protocol"; el tipo C está basado en la propuesta de EPC Global Class1 Gen2. Los tipos A y B están publicados; el tipo C está en vías de redacción. Los tres tipos no son interoperables los unos con los otros.

ISO/IEC 18000-7 - Parameters for Air Interface Communications at 433 MHz (Tecnología desarrollada por el fabricante norteamericano Savi®)

No existe la 18000-5 Part 5, que al principio estaba reservada a la frecuencia de 5,8 GHz, que hasta ahora no se ha solicitado. Todas estas normas están publicadas desde septiembre y octubre de 2004 y, por consiguiente, están disponibles en el AFNOR en Francia y/o en el ISO de Ginebra.

7.3.3 ISO / IEC 18047

La publicación de dichas normas 18000 aún no es suficiente para garantizar la interoperabilidad; aún quedan por realizar pruebas para comprobar la conformidad de los productos disponibles en el mercado.

El ISO ha producido al respecto las normas 18047, que se reparten como las normas básicas, por frecuencia.

Están conformadas por:

ISO/IEC 18047: Information Technology - Automatic Identification and Data Capture Techniques - RFID Conformance Test Methods

ISO/IEC 18047-2 - Parameters for Air Interface Communications below 135 KHz. Publicación prevista en enero de 2006.

ISO/IEC 18047-3 - Parameters for Air Interface Communications at 13,56 MHz. Publicada en septiembre de 2004.

ISO/IEC 18047-4 - Parameters for Air Interface Communications at 2.45 GHz.

ISO/IEC 18000-6 - Parameters for Air Interface Communications at UHF (from 860 to 960 MHz).

ISO/IEC 18000-7 Part7 - Parameters for Air Interface Communications at 433 MHz.

7.3.4 ISO/IEC 159

Estas tres normas aseguran la coherencia entre órdenes de lectura y gestión de datos.

ISO/IEC 15961: Information Technology - Automatic Identification and Data Capture Techniques - RFID for item Management - Host Interrogator - Tag functional commands and other syntax features

ISO/IEC 15962: Information Technology - Automatic Identification and Data Capture Techniques - RFID for item Management - Data Syntax

ISO/IEC 15963: Information Technology - Automatic Identification and Data Capture Techniques - RFID for item Management - Unique identification of RF Tags and Registration Authority to manage the Uniqueness

Esta última norma asegura que todos los chips que formen una etiqueta de radiofrecuencia tengan

un número unívoco, e indica un organismo encargado de gobernar dicha univocidad, por ello, va a permitir la trazabilidad de cada etiqueta.

7.3.5 ISO/IEC 19762

Cabe añadir, en su forma más adecuada, una última norma, que atañe al vocabulario utilizado en todas las normas ISO que se ocupan de RFID, y que representa, con las normas que se han detallado hasta ahora, la base completa de las normas ISO para garantizar la interoperabilidad.

ISO/IEC 19762: Information Technology - Automatic Identification and Data Capture Techniques - Harmonized Vocabulary

ISO/IEC 19762-1 - General Terms Relating to AIDC
ISO/IEC 19762-2 - Radio-Fréquency Identification (RFID)

7.3.6 ISO/IEC 18046

En febrero de 2005 se publicó un "Technical Report" (Informe Técnico), que permite a los integradores de soluciones RFID encontrar los sistemas que atienden las necesidades de sus clientes, sobre la base de prestaciones comprobadas.

Ello va a permitir también a los propios usuarios escoger entre soluciones diferentes. Gracias a la interoperabilidad todos los lectores que cumplen con la norma 18000 pueden leer todas las etiquetas RFID que son igual de conformes con la misma norma.

Sin embargo, dicha interoperabilidad no significa en absoluto que todos los sistemas disponibles en el mercado tengan las mismas prestaciones, perfectamente iguales las unas a las otras. La captura de la información va a garantizarse en todos los casos, pero no la distancia y la rapidez de lectura, por ejemplo, o la propia tasa de lectura en un medio electromagnético concreto.

ISO/IEC 18046: Information Technology - Automatic Identification and Data Capture Techniques - RFID Performance Test Methods

7.3.7 ISO/IEC 24729

La primera se refiere a la publicación de una especie de guía para la puesta en marcha de la

tecnología RFID, tanto en lo que se refiere a las etiquetas, como el reciclado de los chips, o la instalación de las antenas. La misma tiene por objeto ayudar a los usuarios a considerar el mundo real en el que van a funcionar.

ISO/IEC 24729: Information Technology - Automatic Identification and Data Capture Techniques - Radio frequency for item management - Implementation Guidelines

ISO/IEC 24729-1 - RFID – Disponibilidad de tarjetas.

ISO/IEC 24729-2 - Reciclaje de etiquetas RFDI.

ISO/IEC 24729-3 - RFID Instalación del interrogador de la antena

7.3.8 Otros estándares ISO/IEC

ISO/IEC 10536 Identification cards – Contactless integrated circuit cards

Para tarjetas de identificación inteligentes que operan a 13,56 MHz. Describe sus características físicas, dimensiones localización de las aéreas de interrogación, las señales electrónicas y los procedimientos de reset, las respuestas de reset y el protocolo de transmisión.

ISO/IEC 14443 Identification cards – proximity integrated circuit cards

Desarrollado para tarjetas de identificación inteligentes con rango superior a un metro, utilizando la frecuencia 13,56 MHz. Describe las características físicas, la interfaz aérea, la inicialización y anticolisión, y el protocolo de transmisión.

ISO/IEC 15693 Contactless integrated circuit cards – Vicinity cards

Se desarrollan las características físicas, la interfaz aérea y los protocolos de transmisión y anticolisión para tarjetas sin contacto con circuitos integrados en la banda HF (13,56 MHz).

ISO/IEC 19762: Harmonized vocabulary – Part 3: radio-frequency identification

Este documento proporciona términos generales y definiciones en el área de la identificación automática y técnicas de captura de datos, con secciones especializadas en varios campos técnicos, al igual que términos esenciales para ser usados por usuarios no especializados en comunicaciones. La parte 3 es la que hace referencia a la tecnología RFID.

ISO/IEC 18001 RFID for Item Management - Application Requirements Profiles

Proporciona el resultado de tres estudios para identificar aplicaciones y usos de la tecnología RFID con gestión a nivel unidad de artículo, con una clasificación resultante según diferentes parámetros

operacionales, incluyendo el rango de operación, tamaño de la memoria, etc. También una breve explicación de los temas asociados con los parámetros de distancias, número de etiquetas dentro del campo de lectura, etc. Se incluye una clasificación de los tipos de las etiquetas según las aplicaciones.

7.4 EPCGlobal Network

El EPC, siglas de Código Electrónico de Producto (Electronic Product Code), nace de las manos de EPCglobal, un consorcio formado por EAN International (European Article Numbering) el cual tiene 101 organizaciones miembro, representadas en 103 países y UCC (Uniform Code Council) propietario del UPC (Universal Product Code), presente en 140 países y ahora llamado GS1 US.

La intención de EPCglobal al crear el EPC no fue otra que la de promover la EPCglobal Network, un concepto de tecnología que pretende cambiar la actual cadena de suministro por otra con un estándar abierto y global, que permita la identificación en tiempo real de cualquier producto, en cualquier empresa de cualquier parte del mundo.

La EPCglobal Network ha sido desarrollada por el Auto-Id Center, un equipo de investigación del MIT (Massachussets Institute of Technology) que cuenta con laboratorios por todo el mundo. Dicho desarrollo fue llevado a cabo en más de 1000 compañías de alrededor del mundo.

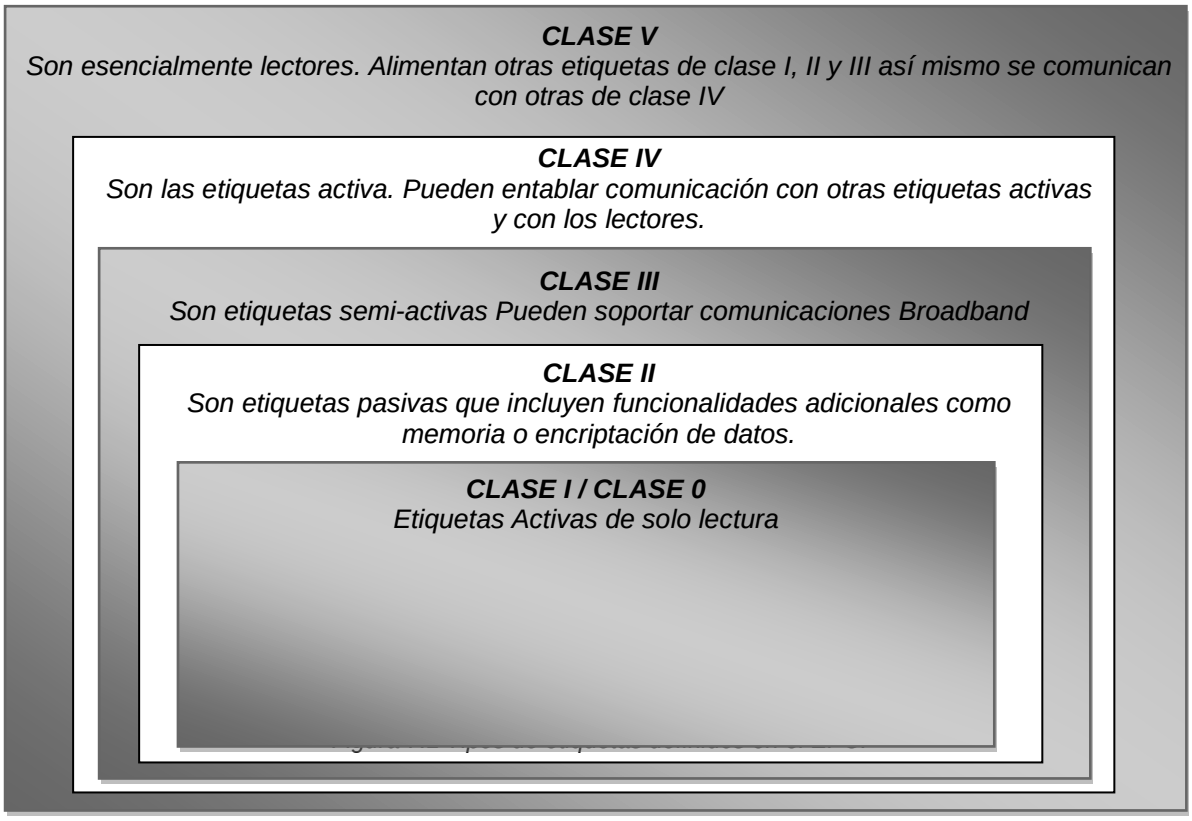
Así mismo, actualmente, todo estándar que desarrolla EPCglobal pasa por la supervisión de la ISO (International Standards Organization), con la única condición de que los estándares concretos que crea ISO sean ratificados y usados en los que cree EPCglobal.

Una vez conocemos de donde proviene el EPC, vamos a hacer un pequeño estudio sobre el estándar para ver qué ventajas e inconvenientes nos proporciona.

Las especificaciones del EPC se pueden dividir en:

- Especificaciones para las etiquetas, referentes a los datos almacenados en ellas, a los protocolos de comunicación con el lector y la parte de RF que permite la comunicación.
- Especificaciones para los lectores: protocolo para el interfaz aire y comunicaciones lógicas con las etiquetas.

El estándar EPC divide las etiquetas usadas en seis tipos diferentes, dependiendo de su funcionalidad, como a continuación se muestra:



7.1 Tipos de etiquetas definidos en el EPC

En Enero de 2005, EPCglobal publicó las especificaciones de la última versión de EPC, el ECP Generación 2, versión 1.0.9.

Esta última publicación está llamada a ser el estándar adaptado a nivel mundial en el uso de los sistemas de RFID ya que se ha realizado para cumplir con las necesidades de los consumidores. Para poder suplir las necesidades mencionadas EPCglobal, además de incluir especificaciones no observadas en otras regulaciones realizadas anteriormente, ha pretendido homogeneizar los principales estándares existentes.

En la siguiente tabla podemos observar los estándares que se tienen como prerrequisito en EPC Gen2, los más importantes existentes en la actualidad. Un dato muy importante es que se incluye la norma EN 302 208 de la ETSI, cosa que representa un gran paso para una estandarización única entre Europa y USA, es decir: él EN 302 208 y el EPC Generación 2 se complementan el uno al otro.

EPCglobal™: EPC™ Tag Data Standards
EPCglobal™ (2004): FMCG RFID Physical Requirements Document (draft)
EPCglobal™ (2004): Class-1 Generation-2 UHF RFID Implementation Reference (draft)
European Telecommunications Standards Institute (ETSI), EN 302 208: Electromagnetic compatibility and radio spectrum matters (ERM) – Radio-frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W, Part 1 – Technical characteristics and test methods
European Telecommunications Standards Institute (ETSI), EN 302 208: Electromagnetic compatibility and radio spectrum matters (ERM) – Radio-frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W, Part 2 – Harmonized EN under article 3.2 of the R&TTE directive
ISO/IEC Directives, Part 2: Rules for the structure and drafting of International Standards
ISO/IEC 3309: Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure
ISO/IEC 15961: Information technology, Automatic identification and data capture – Radio frequency identification (RFID) for item management – Data protocol: application interface
ISO/IEC 15962: Information technology, Automatic identification and data capture techniques – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions
ISO/IEC 15963: Information technology — Radiofrequency identification for item management — Unique identification for RF tags
ISO/IEC 18000-1: Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized
ISO/IEC 18000-6: Information technology automatic identification and data capture techniques — Radio frequency identification for item management air interface — Part 6: Parameters for air interface communications at 860–960 MHz
ISO/IEC 19762: Information technology AIDC techniques – Harmonized vocabulary – Part 3: radio-frequency identification (RFID)
U.S. Code of Federal Regulations (CFR), Title 47, Chapter I, Part 15: Radio-frequency devices, U.S. Federal Communications Commission

Tabla 7.2 Los documentos aquí listados son de obligado cumplimiento para poder aplicar la especificación EPC Generation 2.

Las especificaciones de la capa física del EPC Gen2 establecen que en las comunicaciones del lector a la etiqueta deben usarse modulaciones de doble banda lateral ASK (*double sideband amplitude shift keying – DSB-ASK*), simple banda lateral ASK (*simple sideband amplitude shift keying – SSB-ASK*) o de reverso de fase ASK (*phase reversal amplitude shift keying – PR-ASK*), con una codificación de pulsointervalo (*pulse-interval encoding - PIE*). El lector esperará una respuesta de backscatter (*backscattering reply).*

En la comunicación de la etiqueta al lector se deberá enviar una señal no modulada codificada en formato FM0 o código Miller.

En ambos casos el método usado para comunicarse es Half Dúplex.

Para proceder a la identificación de las etiquetas que se encuentran dentro del radio de acción del lector existen 3 operaciones básicas:

- *Select*. Esta operación permite al lector poder 'ver' qué población de tags hay disponible en su rango de acción. Se puede decir que este proceso es equivalente a una Select realizada en una sentencia Sql para bases de datos, de ahí su nombre.

- *Inventario*. Es la operación que nos permite identificar las etiquetas. El proceso de inventario se inicia cuando el lector manda un comando *Query.* Entonces uno o más tags pueden responder a esta petición. El lector detecta una única respuesta de un tag y entonces interroga a éste para que le proporcione el código PC (*Protocol Control)*, el código EPC y el CRC-16. Este proceso comprende varios comandos y se realiza en una única sesión a la vez.

- *Acceso*. El proceso de acceso comprende varias operaciones de comunicación con la etiqueta (lectura y/o escritura). Una única etiqueta debe ser identificada antes de iniciar el proceso de acceso a la misma.

De todos modos, el proceso de comunicación entre el lector y la etiqueta es mucho más complicado de lo que en un principio puede parecer. En la figura que tenemos a continuación podemos ver un diagrama de estados de una etiqueta. Estos estados representan la situación en la que se encuentra una etiqueta en cada posible momento de una comunicación con el lector.

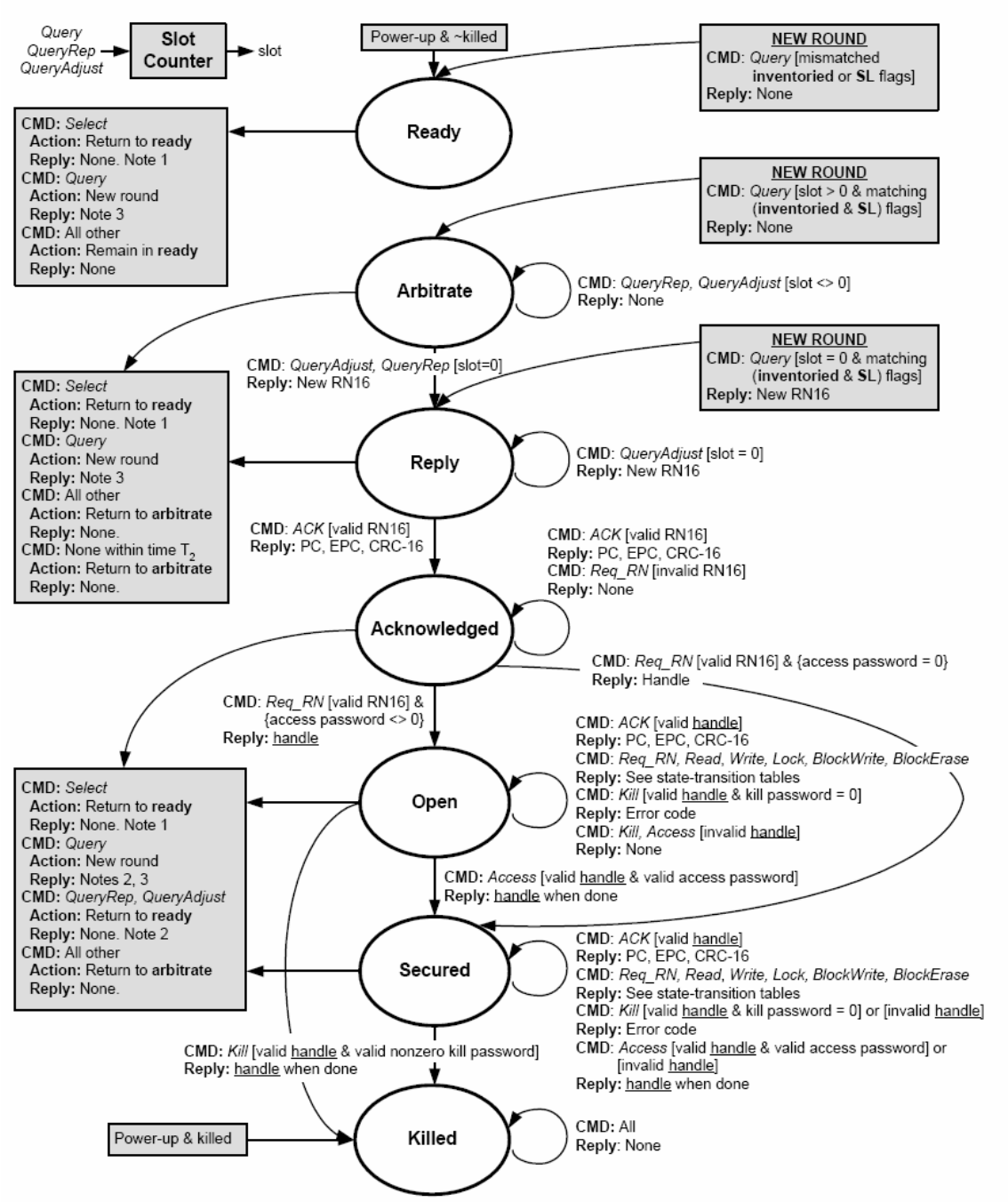


Figura 7.2 Diagrama de estados de una etiqueta que cumple EPC Generation 2.

7.5 EN 302 208

Actualmente existen limitaciones en Europa en lo que al uso de RFID, dentro de la banda UHF, respecta ya que por el momento se encuentra limitado a frecuencias entre los 869.40 y los 869.65 MHz. debiendo cumplir la norma EN 300 220, la cual no contempla las necesidades de RFID en la banda UHF, con una potencia radiada equivalente menor a 500mW y un ciclo de trabajo inferior al 10%.

La existencia de estas limitaciones dentro de la banda UHF, junto a las necesidades de un mercado que permita la libre circulación de equipos de RFID comunes para los países de la Unión Europea y la no armonización del espectro ha motivado que, en mayo de 2005, la ETSI publicara un nuevo estándar. El EN 302 208.

Este nuevo estándar aumenta la banda frecuencial en la cual pueden trabajar los sistemas RFID hasta los 3MHz. (desde los 865.00MHz. hasta los 868.00MHz.), con una potencia radiada equivalente como vemos en la siguiente figura:

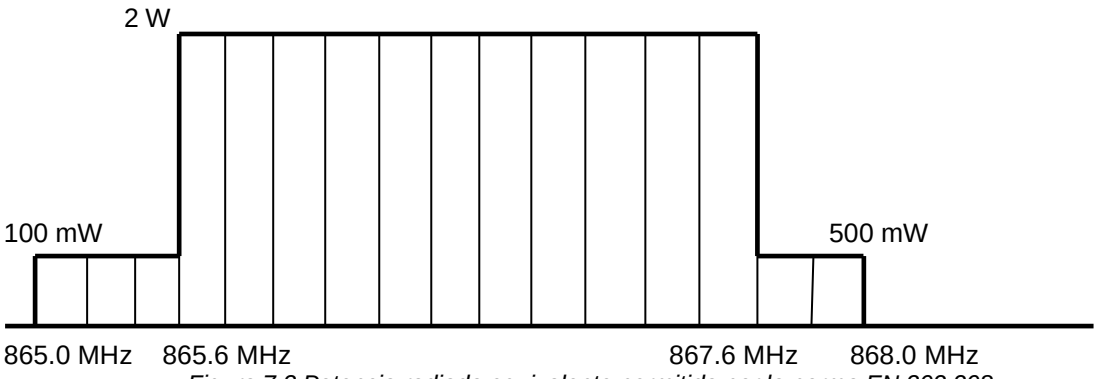


Figura 7.3 Potencia radiada equivalente permitida por la norma EN 302 208.

Dentro de estas ventajas que proporciona la EN 302 208 también existen ciertas condiciones para el uso general de RFID en Europa. Una de ellas es el modo de trabajo que deben tener las etiquetas: “listen before talk”, es decir, el tag deberá permanecer en modo ‘idle’ hasta que el lector no le solicite ningún tipo de información. Esto se puede considerar totalmente lógico si tenemos en cuenta que estamos tratando con etiquetas pasivas, las cuales no tienen una fuente de alimentación propia y, por lo tanto, deben optimizar la energía de la que disponen (campo magnético generado por el lector).

Otras de las condiciones que se incluyen dentro de esta norma de la ETSI son:

- El uso de sub-bandas de 200kHz
- Tiempo de escucha mayor de 5ms.

- Tiempo máximo continuado de transmisión de 4 segundos
- Una pausa obligada de 100ms entre transmisiones repetidas en la misma sub-banda o mover inmediatamente a otra sub-banda que esté libre la transmisión a realizar.

8. Implementación de un Sistema de Control de Acceso RFID

Recordemos que uno de los objetivos de este trabajo es realizar una implementación de una solución efectiva de control de acceso de bajo costo basado en la tecnología de Identificación por Radio Frecuencia utilizando componentes existentes en el mercado que cumplan con las normas internacionales de calidad ISO y desarrollar una aplicación de software para la gestión de las tags. Es por tal motivo que el presente capitulo presenta un análisis de las consideraciones generales para la implementación de un sistema de control de acceso RFID a edificios, así mismo se presenta una propuesta de solución con dicha tecnología empleando un lector Phidget 1023 LF de 125KHz con tags Phidget Ultra delgadas y tipo botón que trabajan a la misma frecuencia.

8.1 Consideraciones

Cabe mencionar que para la implementación de cualquier tipo de tecnología sobre el control de acceso a instalaciones de cualquier indote se deben conocer las políticas de seguridad de la organización así como el proceso que debe seguir el personal o los visitantes externos para la entrada y salida a las instalaciones.

A continuación se describe el procedimiento para permitir el acceso del personal a instalaciones escolares

El ejemplo de la aplicación que en este trabajo se maneja es una aplicación de control de acceso generalizada, es decir no está basada concretamente a un tipo especifico de instalaciones, sin embargo este podría utilizarse para una aplicación escolar ya que el diseño puede acoplarse fácilmente a una de estas características. Sin embargo me parece muy importante mencionar el procedimiento de acceso de personal a instalaciones escolares puesto que este tipo de instalaciones es donde existen muchos más cuestiones que en otros tipos de controles de acceso.

En una escuela cada alumno inscrito debe contar con una credencial personal emitida por la institución educativa a la que pertenece, dicha credencial debe ser actualizada cada determinado periodo de tiempo conforme a las políticas de la institución. Normalmente estas credenciales además de los datos personales del alumno contienen su numero de matricula y fotografía.

Dichas credenciales son el documento que acredita a los alumnos como pertenecientes a alguna escuela especifica y además de ser el requisito para el ingreso al plantel son utilizadas para realizar trámites internos en las instalaciones educativas como son el préstamo de libros de las bibliotecas, ingreso a los laboratorios de cómputo u otros, entre otros tramites.

Una vez analizado el proceso de control de acceso que se lleva a cabo para permitir la entrada de estudiantes a las instalaciones escolares se puede observar que cuenta con las siguientes desventajas:

- Si el alumno no cuenta con la credencial que lo acredita como estudiante de ese plantel lo más lógico es que no pudiera tener acceso al mismo hasta que no cuente con un documento que indique que esta en proceso su repuesto de credencial de estudiante.

  Sin embargo esto no sucede así y por lo contrario cuando es este el caso normalmente el alumno tiene acceso mostrando una impresión de horario de clases, él cual no garantiza que los datos ahí presentes pertenezcan a él ya que este documento no cuenta con fotografía ni con algún sello de la institución que garantice lo anterior.

  Por tal motivo cualquier persona que cuente con una impresión de un horario de clases o cualquier otro documento que no contenga fotografía o algún sello de la institución educativa puede tener acceso a las instalaciones sin importar cuales sean sus intenciones una vez estando dentro de las mismas.

- En el mayor de los casos estas credenciales están impresas en materiales como el pvc y el poli carbonato que facilitan la invisibilidad de los datos del estudiante al que pertenece.

- Pueden ser falsificadas con cierto grado de facilidad ya que si alguna persona cuenta con datos reales de algún estudiante esta puede realizar varias copias con los mismos datos y así pueden ingresar varias personas con la “misma credencial” y realizar tramites usando estos datos.

- Tramites repetitivos (en el llenado de formatos para el préstamo de libros y/o acceso a los laboratorios)

Como se puede observar estas desventajas pueden acarrear muy diversos problemas que van desde la entrada a las instalaciones al plantel por personas ajenas a él poniendo en riesgo la integridad de los estudiantes y del personal que ahí labora así como las propias instalaciones y el activo con el que se cuente, hasta la falsificación de datos y el uso de los mismos de manera repetitiva e indebida para la realización de tramites y posible suplantación de identidad.

Uso de RFID para el control de acceso a Instalaciones

Como ya se explico en capítulos anteriores el uso de la tecnología RFID puede y esta dando solución a este tipo de problemas no solo controlando el acceso a instalaciones educativas sino de cualquier índole y además permitiendo y garantizando la autenticidad del personal.

Las principales ventajas de este tipo de tecnologías basadas en el control de acceso son las siguientes:

- *Seguridad en los datos.* En la actualidad los distintos dispositivos RFID utilizan el cifrado de datos, debido a esto los mismos no pueden ser leídos por lectores RFID comunes.
- *Garantía de Identidad.* Debido a que los datos son encriptados y solo pueden ser leídos y modificados por lectores/escritores que cumplan con ciertas normas de calidad y autorizadas por la organización le dan un alto grado de confiabilidad a los datos de cada Tag.

  Existes sistemas de Control de acceso basados en esta tecnología que se completan con sistemas biométricos y de reconocimiento facial los cuales refuerzan la seguridad de los datos.

- *Posibilidad de la modificación de los datos contenidos en el tag.* Depende de los estándares.

- *Compatibilidad en el desarrollo de software para la gestión del personal*. Por ejemplo existen en el mercado soluciones de software que permiten integrar manejo de tecnología RFID algunas son Microsoft Biztalk, Oracle y Sybase. Así mismo los lenguajes de programación mas utilizados en el mundo como Microsoft .Net y Java permiten desarrollar software para RFID.

- *Costos.* En descenso a medida que se aplican los últimos avances tecnológicos.
- *Componentes respaldados por estándares de calidad.* Existen diferentes estándares universalmente aceptados, y relacionados con la banda de frecuencia utilizada, que como ya hemos visto, determina el tipo de sistema RFID. Los dos estándares principales son el estándar EPC y el estándar ISO.

- *Vida útil*. Al no haber necesidad de contacto físico ni de baterías, la vida útil de las etiquetas pasivas es muy grande. Las etiquetas activas tienen limitada su vida útil a la duración de su batería.

- *Tamaño*. En general, desde el tamaño de un botón o un caramelo hasta el tamaño de un paquete de tabaco.

- *Posibilidad de darle varios usos a una misma Tag*: Estas tarjetas son cada vez más funcionales, pudiendo permitir no sólo el acceso, sino también a máquinas expendedoras o para pagos pequeños, por ejemplo en una cafetería de una escuela o empresa.

- *Capacidad de los lectores de leer múltiples tags al mismo tiempo*. A diferencia de otras tecnologías como el código de barras o cinta magnética un lector RFID puede leer varias tarjetas al mismo tiempo y distancias diferidas, claro todo depende de los estándares utilizados.

Este tipo de soluciones pueden complementarse y conjugarse con otras tecnologías para reforzar el nivel de seguridad en una primera instancia sin embargo también pueden incrementar el nivel de productividad, gestión y movimiento de personal entre otras posibilidades.

8.2 Dispositivos

Es muy importante mencionar que para la adquisición del lector y las Tags RFID se tuvo que realizar el pedido vía web (*www.phidgets.com*) ya que en nuestro país no existe un distribuidor que surta este tipo de componentes de manera individual.

Existen infinidad de fabricantes en el mundo de este tipo de dispositivos sin embargo la elección de esta marca fue por la compatibilidad del lector con la tecnología .Net de Microsoft y básicamente por tener un precio razonablemente bajo a comparación de otras marcas.

A continuación se hace una descripción de los componentes utilizados para la realización de esta solución.

- Lector RFID.- Se utilizo un lector marca Phidget 1023 LF de 125KHz cumple con la norma ISO EM4102. La tabla 8.1 muestras sus características técnicas. Tiene la función de hacer las lecturas de las tags, y enviar la información obtenida a la PC. Establece una comunicación punto a punto con el equipo de computo por medio de una interfase USB 2.0, trabajando con una tasa de transferencia de 9600Bit/.Permite la lectura de etiquetas a una distancia de 10cm aprox. Dependiendo del tipo de tarjeta. Es únicamente de lectura no permite la escritura en las Tags.

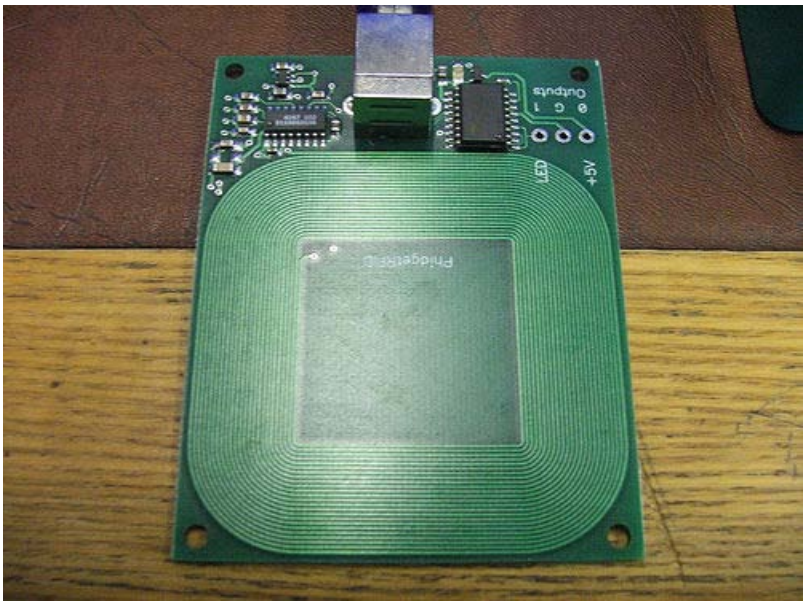


Figura 8.1 Lector RFID Phidget 1023

- Tags RFID.- Se manejaron tags de la marca Phidget de 125KHz, una tag tipo tarjeta de identificación y otra encapsulada en un botón de plástico que puede ser usada como llavero. Recuerde que el papel que este dispositivo tiene es guardar en su interior el número de identificación del usuario, el cual intercambiara con el lector al ser leídos por este.

Características técnicas del lector	
Frecuencia de Resonancia de Antena	125kHz - 140kHz
Protocolo de comunicación con Tags	EM4102
Frecuencia de lectura	LF 125KHz
Ritmo de actualizaciones de lectura	30 updates / second
Fuente de Alimentación	5VDC
Terminal de cable recomendada	16 - 26 AWG
Tipo de Tags soportadas	Cualquier que soporte el protocolo ISO EM4102 (La forma y el tamaño no importa)
Plataformas Soportadas	Windows 2000/XP/Vista, Windows CE, Linux y Mac OS X
Lenguajes de programación Soportados	VB6, VB.NET, C#.NET.

Tabla 8.1 Características técnicas del lector Phidget 1023

Figura 8.2. Tipos de tags utilizadas

Características de las Tags	
Frecuencia de operación	125 KHz
Transferencia de datos	106 Kbits/s
Soporta Anticolisión	Sí
Tiempo de lectura	35ms

8.2 Características de los tags utilizados

- Computadora personal.- Se utilizo una PC con Procesador AMD Athlon 64 X2 Dual Core 3800+ a GHz, 2GB de RAM y 180 en HD. Este es el responsable de la interacción entre el hardware RFID y el software. Permite la recolección de la información desde el lector RFID, la procesa mediante el software y realiza la gestión de la misma.
- Lenguaje de Programación.- Por ser uno de los lenguajes más usados a nivel global y por el potencial del mismo se utilizo Microsoft .Net, además de que es uno de los pocos lenguajes que en la actualidad permite la programación de aplicaciones RFID junto con Java.
- Manejador de Base de Datos.- Puesto que se trabajo bajo la plataforma .Net se opto por utilizar Microsoft SQL Server 2005 Express Edition aunque .Net puede adecuarse a cualquier otro manejador de bases de datos como MySQL, Oracle, Informix u otros.

Códigos de Error del Lector

La siguiente tabla muestra los códigos de error con los que cuenta el lector. Estos códigos de error pueden aparecer durante la lectura de las Tags. Dichos códigos el fabricante los muestra al público para que puedan gestionarse durante la codificación de aplicaciones que utilicen este hardware RFID

Códigos de Error	
‘E’	Formato Invalido de Clave
‘F’	Falla en el lector
‘N’	Sin etiquetas en el rango de lectura
‘X’	Autenticación fallida

Tabla 8.3 Códigos de Error del lector Phidget proporcionados por el fabricante

Comunicación con el lector

Para poder desarrollar la aplicación RFID que gestione las etiquetas se uso los archivos DLL que contiene las funciones para poder inicializar la comunicación con el lector. En la figura 8.4 se muestran las funciones que conforman el archivo DLL para poder establecer la comunicación con el dispositivo.

Dicho ensamblado está compuesto por 44 funciones y 30 eventos los cuales están totalmente encriptados para que el desarrollador no pueda alterarlos.

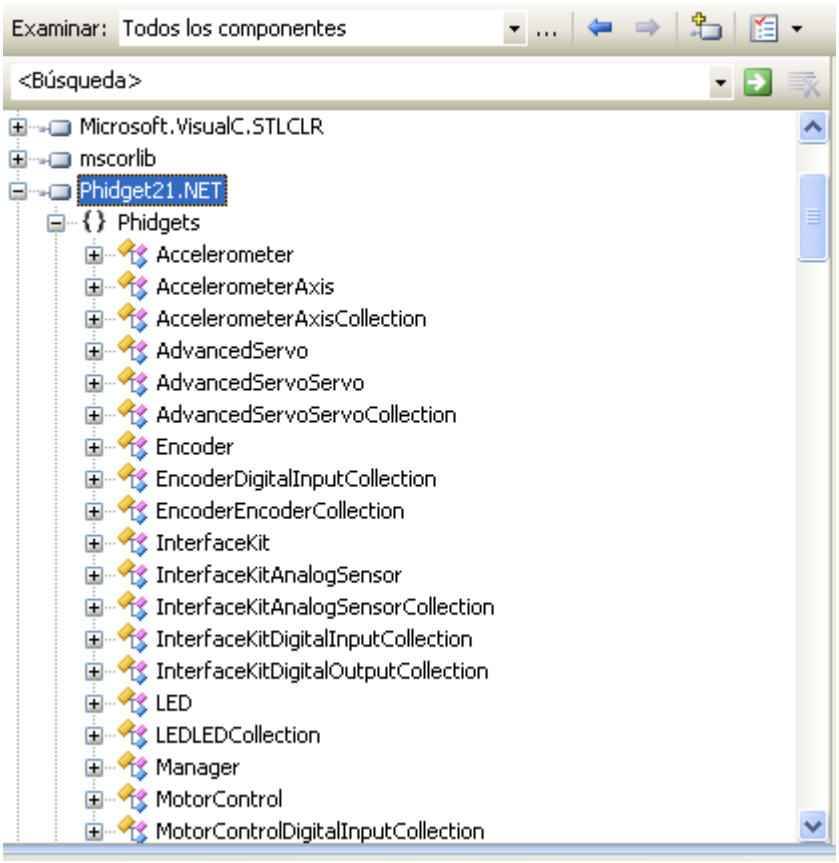


Figura 8.3 Funciones del ensamblado Phidget21.NET proporcionado por el fabricante para el desarrollo de soluciones RFID

8.3 Características de funcionamiento de la Aplicación

Un sistema de control de acceso funciona de la siguiente manera:

- Se codifica la tarjeta con chip RFID con un código identificativo único (normalmente desde fabrica). Al aproximar esta tarjeta al lector, transmite tal código mediante ondas de radio al lector. El código único del chip evita la falsificación de la tarjeta y posibilita la trazabilidad de personas dentro de las instalaciones.
- Los lectores o terminales transmiten los datos a un ordenador conectado para su autentificación.
- El software comprueba la información mandada y avisa al torniquete para conceder o denegar el paso, o bien ficha la hora de entrada o salida del empleado o alumno y la guarda en su base de datos.

Nota. En esta implementación no se utilizo un torniquete como tal, se uso un diodo emisor de luz (LED) incrustado en la tarjeta del lector RFID para que al momento de ser leída una Tag y se identificara el LED encendiera lo que indica que autoriza el pase a las instalaciones. En caso contrario si el LED se encuentra apagado es porque no se ha detectado Tag alguna o no ha sido autenticada por el lector. Cabe mencionar que para que el torniquete reciba la señal de abrir se necesita una tarjeta RS232/RS485 la cual procesa el Byte recibido directamente de la aplicación y la envía al torniquete.

8.4 Desarrollo de la Aplicación RFID

A continuación se explica brevemente las consideraciones que se tomaron para desarrollar la aplicación RFID:

- Primeramente se debe establecer la comunicación de la PC con el lector.
- Conexión con la base de Datos
- Lectura de Tarjetas RFID
- Autenticidad
- Permitir Acceso

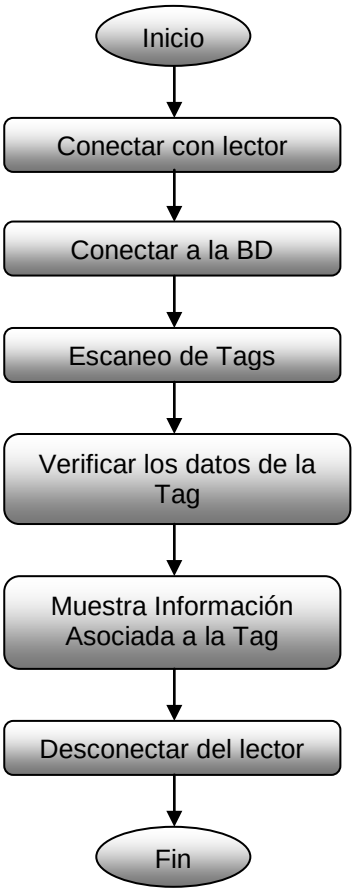


Figura 8.4 Diagrama de flujo que representa el flujo básico de trabajo de una aplicación RFID

8.4.1 Plataforma e Interfaz Grafica

Para realizar la parte que relaciona el sistema con el usuario, se requiere un software que permita desarrollar aplicaciones complejas pero con una interfaz sencilla y amigable y que además se acople perfectamente a la plataforma del sistema operativo de Microsoft

Teniendo en cuenta lo anterior, se seleccionó Visual C#.Net, el cual es un lenguaje basado en objetos con propiedades y métodos, entre otras características. Este es un lenguaje de programación visual, también llamado lenguaje de cuarta generación; esto quiere decir que un gran número de tareas se realizan sin escribir código, simplemente con operaciones gráficas realizadas con el ratón, sobre la pantalla.

Así mismo se opto por utilizar el IDE (Integrated Development Environment) de Microsoft Visual Studio.Net 2008 para facilitar la codificación y compilación de la aplicación.

Visual C# está orientado a la realización de software para Microsoft Windows, pudiendo incorporar todos los elementos de este entorno informático: ventanas, botones, cajas de diálogo y de texto, botones de opción y de selección, barras de desplazamiento, gráficos, menús, etc.

En el desarrollo del código se destacan tres componentes importantes que se deben implementar para integrar el hardware, el software, el servidor con las bases de datos y el usuario.

Antes de comenzar hay que señalar que no es la finalidad de este trabajo explicar cómo realizar una base de datos en SQL Server mucho menos como programar en el lenguaje .Net sin embargo se explicará el código más importante que se desarrollo para la aplicación RFID.

Cuando los datos son adquiridos por Visual C# desde el lector RFID, estos se utilizan para realizar procesos relacionados con las base de datos, donde se mantiene el registro de las personas.

Esta base de datos se encuentra en la misma computadora donde se ejecuto la aplicación sin embargo se puede configurar para que la base de datos se conecte desde otro servidor, es decir que la aplicación sea totalmente distribuida.

El software desarrollado para la aplicación realiza todas sus transacciones a través de una interfaz grafica amigable; es por esto que se hace necesario manejar las bases de datos por medio de código y la comunicación entre Visual C# y una base de datos basada en el lenguaje SQL, se hace utilizando objetos ADO.Net (Active Data Object.Net).

ADO.Net contiene la colección de objetos para crear una conexión a bases de datos y leer datos desde tablas, trabajando como una interfaz hacia la fuente de datos. Sin embargo, no se comunica directamente con la base, sino que accede a ella a través de una interfaz intermediaria, llamada DB (OLE Data Base).

En general, después de crear una conexión a la base de datos, se puede ignorar la existencia de OLE DB, debido a que este driver hace todo su trabajo en "background". Existen dos maneras para que el proveedor OLE DB brinde acceso a una base de datos: directamente, en la cual se accede mediante un driver ODBC (Open Data Base Conectivity) o indirectamente, modo en el que se accede mediante un driver OLE DB nativo.

Esta colección de objetos permite acceso a datos remotos y los usuarios de ADO.Net pueden transmitir datos a través de HTTP a un cliente, trabajar con dichos datos y devolverlos al servidor HTTP de nuevo.

Los objetos utilizados en los métodos de conexión y sus propiedades se describen en la siguiente tabla.

Métodos	Descripción
Open	Abre una conexión a los datos
Close	Cierra una conexión y cualquier objeto dependiente
Execute	Ejecuta una consulta, un procedimiento almacenado, una sentencia SQL.
BeginTransaction	Inicia una nueva transacción
CommitTransaction	Guarda los cambios y termina la transacción
ConnectionString	Contiene la información usada para establecer una conexión a una base de datos.

Tabla 8.4 Objetos SQL

La implementación de esta aplicación se fundamenta en dos procesos; el primero es crear un objeto ADODB (Active Data Object Data Base) del tipo connection usando la sintaxis,

Sqlconnection conexion = new Sqlconnection ();

para el que, de acuerdo al uso de sus atributos, abre el servidor SQL, selecciona la base de datos, se registra autenticándose con forme al usuario que tiene acceso al sistema operativo en la cual se esté alijada la base de datos. Un ejemplo el código que establece la conexión con una base de datos es el siguiente:

```
string cadena = @"Data Source =.\SQLEXPRESS; initial catalog = Northwind; Integrated
Security=true";
SqlConnection conexion = new SqlConnection(cadena);
```

8.5 Base de Datos

Para manipular bases de datos existen aplicaciones como Microsoft Access, el cual tiene deficiencias en robustez y seguridad en comparación con SQL Server también de Microsoft. Siendo este un proyecto pensado para una aplicación de seguridad, encargado de manejar alto flujo de datos, se hizo necesario indagar sobre otra alternativa que satisficiera lo anterior. Por esto se trabajó con el lenguaje de consulta estructurado SQL, el cual es un lenguaje de base de datos normalizado, para crear y manipular directamente bases de datos así como hacer consultas SQL en bases de datos remotas cliente-servidor.

El lenguaje SQL está compuesto por comandos, cláusulas, operadores y funciones de agregado. Estos elementos se combinan en las instrucciones para crear, actualizar y manipular las bases de datos.

8.5.1 SELECT

La sintaxis básica de una consulta de selección es la siguiente:

SELECT Campos FROM Tabla;

En donde campos es la lista de campos que se deseen recuperar y tabla es el origen de los mismos, por ejemplo:

SELECT Nombre, Teléfono FROM Clientes;

Esta consulta devuelve un recordset con el campo nombre y teléfono de la tabla clientes. Si no se incluye ninguno de los predicados se asume ALL. El Motor de base de datos selecciona todos los registros que cumplen las condiciones de la instrucción SQL. No es conveniente abusar de este predicado ya que obligamos al motor de la base de datos a analizar la estructura de la tabla para averiguar los campos que contiene, y es mucho más rápido indicar el listado de campos deseados.

En cuanto al manejo de la información en SQL se utilizan las consultas de acción que son aquellas que no devuelven ningún registro y son las encargadas de acciones como añadir, borrar y modificar registros.

8.5.2 DELETE

Crea una consulta de eliminación que elimina los registros de una o más de las tablas listadas en la cláusula FROM que satisfagan la cláusula WHERE. Esta consulta elimina los registros completos, luego no es posible eliminar el contenido de algún campo en concreto.
Su sintaxis es:

DELETE FROM Tabla WHERE criterio

Una vez que se han eliminado los registros utilizando una consulta de borrado, no puede deshacer la operación.

8.5.3 INSERT INTO

Agrega un registro en una tabla. Se la conoce como una consulta de datos añadidos. Esta consulta puede ser de dos tipos: Insertar un único registro ó Insertar en una tabla los registros contenidos en otra tabla.

Insertar un único Registro

En este caso la sintaxis es la siguiente:

INSERT INTO Tabla (campo1, campo2, .., campoN) VALUES (valor1, valor2, ..., valorN)

Esta consulta graba en el campo1, el valor1; en el campo2, valor2 y así sucesivamente. Hay que prestar especial atención a acotar entre comillas simples (') los valores literales (cadenas de caracteres) y las fechas indicarlas en formato mm-dd-aa y entre paréntesis (#).

Para seleccionar registros e insertarlos en una tabla nueva

En este caso la sintaxis es la siguiente:

SELECT campo1, campo2, ..., campoN INTO nuevatabla FROM tablaorigen [WHERE criterios]

Se pueden utilizar las consultas de creación de tabla para archivar registros, hacer copias de seguridad de las tablas o hacer copias para exportar a otra base de datos o utilizar en informes que muestren los datos de un periodo de tiempo concreto.

Insertar Registros de otra Tabla

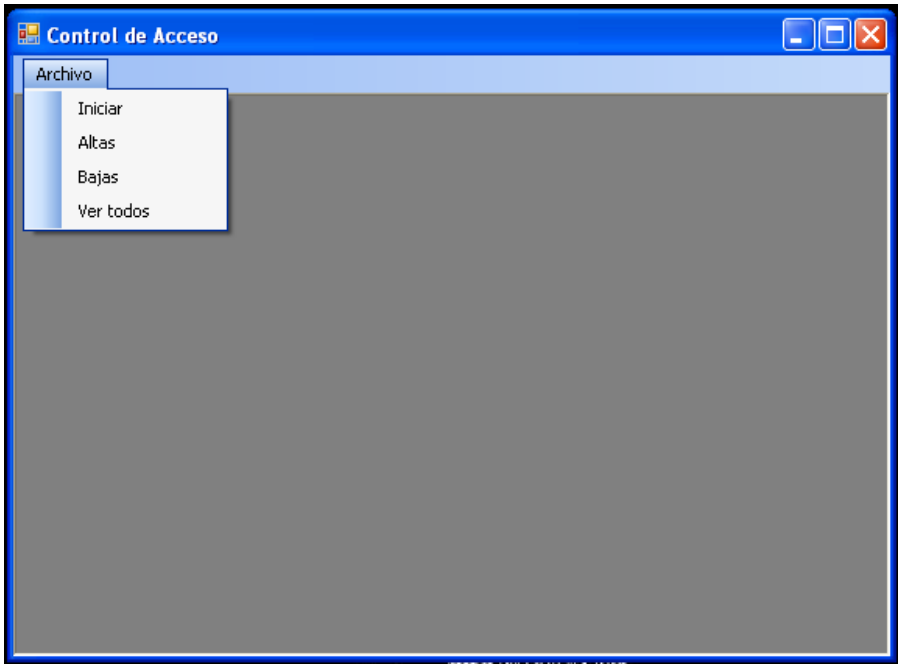
En este caso la sintaxis es:

INSERT INTO Tabla [IN base_externa] (campo1, campo2, ..., campoN)
SELECT TablaOrigen.campo1, TablaOrigen.campo2, ..., TablaOrigen.campoN
FROM TablaOrigen

En este caso se seleccionarán los campos 1,2, ..., n de la tabla origen y se grabarán en los campos 1,2,.., n de la Tabla. La condición SELECT puede incluir la cláusula WHERE para filtrar los registros a copiar.

8.6 Codificando la Aplicación

La aplicación consta de un formulario MDI que será el formulario base de la aplicación y de cuatro formularios más los cuales son: Iniciar, Altas, Bajas, Ver Todos.



8.5 Formulario principal MDI

8.6.1 Estableciendo la comunicación con el lector

En el formulario Iniciar se establece la comunicación con el lector y se realiza la lectura de las Tags.

Para esto se realizo una función llamada rfid_Attach en la misma clase del formulario llamado Iniciar.

Primeramente se deben importar las siguientes directivas:

```
using System.Data;
using System.Data.SqlClient;
using Phidgets;

void rfid_Attach(object sender, AttachEventArgs e)

{
  Phidgets.RFID phid = (Phidgets.RFID)sender;
  lblAttached.Text = "Conectado: " + phid.Name;
  lblSerial.Text = " Serial: " + phid.SerialNumber;
  lblVersion.Text = " Version: " + phid.Version;

}
```

Para usar esta y las demás funciones y establecer conexión con el lector se necesitan 3 variables:

```
RFID rfid1;
string lastRFIDTag;
Int32 TagCtr;
```

Posteriorente en el evento Load del formulario realizamos la conexión para que esta se realialice cuando cargue el formulario Iniciiar.

```
private void Iniciar_Load(object sender, EventArgs e)

{
rfid1 = new RFID();
rfid1.Attach += new AttachEventHandler(rfid_Attach);
rfid1.Detach += new DetachEventHandler(rfid_Detach);
rfid1.RFIDTag += new TagEventHandler(rfid_Tag);
rfid1.RFIDTagLost += new TagEventHandler(rfid_TagLost);
rfid1.op
}
```

Hay que hacer referencia al archivo DLL (Phidget21NET) que se nos proporciono el fabricante del lector el cual almacena las diferentes funciones para programar en .Net con el lector RFID. Este archivo DLL esta encriptado por fabricante y no podemos hacer cambio alguno al archivo.

Las siguientes tres funcionan también tienen mucha importancia con la aplicación ya que la primera rfid_Tag es la encargada de leer las Tags que se encuentren dentro del área de lectura del lector y muestra el código de la misma en una caja de texto previamente establecida en el formulario.

```
void rfid_Tag(object sender, TagEventArgs e)

{
txtTag.Text = e.Tag;
lastRFIDTag = txtTag.Text;
rfid1.LED = true;
   if (txtTag.Text != "")
            {
                picacceso.Visible = true;
            }
}
```

rfid_TagLost es la encargada de mandar la senal al lector y decirle que la tarjeta leida fue dentificada y que debe encender el LED en color verde para indicar que se permite el acceso de la misma

```
void rfid_TagLost(object sender, TagEventArgs e)

{
rfid1.LED = false;
lbPrevRFIDTags.Items.Insert(0,
string.Format("Tag: {0} - {1}", ++TagCtr, lastRFIDTag));
}
```

La ultima funcion basicamente un mensaje de que no se ha establecido la conexion con el lector, pero para que se ande este mensaje se utiliza el evento sender de la funcion el cual debe ser recibido por el evento load del formulario Iniciar.

```
void rfid_Detach(object sender, DetachEventArgs e)
{
lblAttached.Text = "No conectado";
}
```

8.6.2 Conectando la Aplicación a SQL Server 2005 Express Edition

Microsoft ha puesto a disposición de los desarrolladores una amplia base de datos distribuida llamada Northwind que puede descargarse del sitio web de Microsoft sin ningún costo, dicha base de datos esta diseñada para que los programadores puedan explorar todas las funcionalidades con las que cuenta SQL Server 2005 y además de poder usarla en sus aplicaciones sin ninguna restricción .
En este trabajo se aprovecho dicha base de datos base de datos para probar nuestra aplicar RFID, solo se utilizo la tabla Employees y de esta únicamente los siguientes campos:

- Employee ID
- LastName
- FrstName
- Title
- Photo
- TagID

Una vez hecha dicha observación pasamos a explicar el código .Net

Explicando brevemente la interaccion de eventos para que la Tag sea leida, identificada y se muestren los datos de la base de datos asociados tenemos que la conexión se ha establecido previamente en el evento Load del formularo Iniciar mediante la funcion rfid_Attach, ahora bien se aproxima una Tag la cual es leida por la funcion rfid_Tag y se muestra su codigo en una caja de

texto, ahora bien nos falta mostrar los datos de la base de datos asociados con el codigo de la Tag. Para ello primero necesitamos establecer una cadena de conexión y una conexión con SQL Server.

```
string cadena = @"Data Source =.\SQLEXPRESS; initial catalog = Northwind;
Integrated Security=true";
SqlConnection conexion = new SqlConnection(cadena);
```

Esto debe suceder inmediatamente despues de haber leida la Tag,espor este motivo que esta cadena debe decararse dentro del evento text_Chaged de la caja de texto donde se mostrara el codigo de la Tag leida.

Es en este mismo evento donde se debe declarar la sentencia SQL que asociara el codigo Tag con la base de datos. Todo esto mediante el uso de Sqlcommand y un reader para mostrarlos en controles previamente definidos en el frmulario Iniciar.

```
string queryselect = "SELECT * FROM Employees WHERE TagID = '" +
txtTag.Text + "'";

            SqlCommand cmd = new SqlCommand(queryselect, conexion);
            SqlDataReader reader;

            try
            {
                conexion.Open();
                reader = cmd.ExecuteReader();
                if (reader.Read())
                {
                    lblTag.Text = Convert.ToString(reader["TagID"]);
                    lblID.Text = Convert.ToString(reader["EmployeeID"]);
                    lblApe.Text = Convert.ToString(reader["LastName"]);
                    lblNom.Text = Convert.ToString(reader["FirstName"]);
                    lblTitle.Text = Convert.ToString(reader["Title"]);
                    lblencabezado.Text = lblNom.Text + " " + lblApe.Text;


                }
            }
            catch (Exception err)
            {picacceso.Visible = false;
                lblencabezado.Text = err.Message;

            }
            finally
            {
                conexion.Close();
            }
```

Cuando se carga el formulario, limpiamos los datos que pudieran estar llenos. El control temporizador, borra los datos del empleado después de una cierta cantidad de tiempo (por seguridad) en este caso lo establecemos a 3 segundos (debe ser constante en toda la aplicación)

Es decir, cuando un empleado se identifica usando su etiqueta RFID, su información será borrada de la pantalla después de tres segundos

```
private void timer1_Tick(object sender, EventArgs e)
  {
timer1.Interval = 3000;
picfot.Visible = false;
lblTag.Text = "";
lblID.Text = "";
lblApe.Text = "";
lblNom.Text = "";
lblTitle.Text = "";
txtTag.Text = "";
picfoto.Visible = false;
lbPrevRFIDTags.Items.Clear();
lblencabezado.Text = "";
picacceso.Visible = false;
picacceso2.Visible = false;
  }
```

Un punto importante que se debe entender acerca de los lectores de RFID es que cuando se escanea una etiqueta los datos contenidos en ella se envían de manera serial su ID. Por ejemplo, supongamos que una etiqueta con un ID de 0F0296AF3C se coloca cerca del lector. En este caso, el lector podrá enviar continuamente el valor de 0F0296AF3C a la conexión. Para el lector RFID, cada valor comienza con el carácter LF (carácter 10: <10>) y termina con el carácter CR (carácter 13: <13>). Por lo tanto, utilizar el métodos ReadExisting () no garantiza que se lea la etiqueta de identificación completa en su totalidad. Ya que por ejemplo un valor puede ser enviado en cuatro bloques, como este:

<10>0F
029
6AF3
C<13>

La solución seria usar el método ReadLine (), pero no funcionará porque dicho la ReadLine () buscará <13> <10>, en la línea final. Sin embargo, dado que los datos no terminan con <10>, esto hará que la solicitud entre en un bucle infinito.

Y si no borrar el buffer de datos lo suficientemente rápido, puede obtener una serie de datos de cola de esta manera:

<10>
0F
029
6AF3
C
<13>
<10>
04
158D
C82B
<13>

En vez de escribir la lógica de proceso de elaboración de los datos, una forma fácil es anexar todos los datos a un control TextBox (con la propiedad Multilíneas establecida a True).

Como los datos se adjuntan al control TextBox, la primera línea contendrá el carácter LF (<10>) por tanto, la primera línea estará siempre vacía.
De la segunda a la última línea, siempre contendrán la ID de la etiqueta, incluso si la última línea es una cadena vacía.

8.6.3 Formulario Registro de Usuarios

La alta de usuarios a la base de datos se realiza mediante una sentencia Sql, INSERT INTO usando un comando Sqlcommand. Esto se realizo en el botón Insertar del formulario Altas el cual es hijo del formulario base MDI el cual es lavase de la aplicación.
Al igual que en el formulario Iniciar se deben importar las direstivas, system.Data y system.Data.sqlclient así mismo se .debe realizar la conexión como se explico previamente.

```
private void button1_Click(object sender, EventArgs e)

        {
string cadena = @"Data Source =.\SQLEXPRESS; initial catalog = Northwind;
Integrated Security=true";
SqlConnection conexion = new SqlConnection(cadena);
string queryinsert = "INSERT INTO
Employees(TagID,EmployeeID,LastName,FirstName,Title)";
queryinsert += "VALUES (@TagID,@EmployeeID,@LastName,@FirstName,@Title)";

SqlCommand cmd = new SqlCommand(queryinsert, conexion);
int agregado = 0;

        cmd.Parameters.AddWithValue("@TagID", txtTagID.Text);
        cmd.Parameters.AddWithValue("@EmployeeID", txtIDEmpleado.Text);
        cmd.Parameters.AddWithValue("@LastName", txtApellido.Text);
        cmd.Parameters.AddWithValue("@FirstName", txtNombre.Text);
        cmd.Parameters.AddWithValue("@Title", txtCargo.Text);
```

```
try

{

 conexion .Open ();
agregado = cmd.ExecuteNonQuery();
label1.Visible = true;
label1.Text = agregado.ToString() + " " + "Registro Agregado";

}
catch (Exception err)

{
label1.Text = "Error al Tratar de Insertar el Registro";
label1.Text += err.Message;
}

finally

{
conexion .Close ();
}
}
```

Antes de ejecutar cualquier comando sqlcommand se debe abrir laconexion a la base de datos una vez ejecuada elcomando con los datos almacenados en los controles TextBox se cierra la conexión para evitar cualquier perdida de datos o alguna falla. Note que en este formulario no estamos llamando a ningna funcion para gestionar el lector RFID ya que como se menciono solo es necesario para elapartado Iniciar que es el que inicia la lectura de Tags.

8.6.4 Formulario para Baja de Usuarios

De la misma forma para dar de baja usuarios de ejecuta la sentencia Sql, DELETE usando un comando Sqlcommand al cual se le debe señalar la conexión y la sentencia con los cuales se ejecutara.

Sin embargo para dar de baja a un usuario previamente se debe seleccionar que usuario se quiere dar de baja. Para que se pueda seleccionar a uno primeramente se debe realizar un Binding es decir un barrrido de la tabla que almacena los usuarios de los cuales se desea eliminar alguno. Esto se puede realizar de varias formas de las cuales la mas sencilla y amigable es colocar un control combo box que maneje los datos mediante el valor de la PK de la tabla y los coloque en controles como cajas de texto o etiquetas.

```
private void Bajas_Load(object sender, EventArgs e)

{

string cadena = @"Data Source =.\SQLEXPRESS; initial catalog = Northwind;
Integrated Security=true";
SqlConnection conexion = new SqlConnection(cadena);
string query = " SELECT * FROM Employees";
conexion.Open();
SqlDataAdapter adapter = new SqlDataAdapter(query, conexion);
DataSet DS = new DataSet();
adapter.TableMappings.Add("Table", "Employees");
adapter.Fill(DS);
this.dviewmanager = DS.DefaultViewManager;
this.comboBox1.DataSource = this.dviewmanager;

this.comboBox1.DisplayMember = "Employees.TagID";

this.txtIDEmpleado.DataBindings.Add("Text", this.dviewmanager,
"Employees.EmployeeID");
this.txtApellido.DataBindings.Add("Text", this.dviewmanager,
"Employees.LastName");
this.txtNombre.DataBindings.Add("Text", this.dviewmanager,
"Employees.FirstName");
this.txtCargo.DataBindings.Add("Text", this.dviewmanager,
"Employees.Title");

conexion.Close();

}
```

Lo que hacemos es mostrar los códigos de las tags almacenadas en la tabla Employees y que están asociadas a información de usuarios en un control combobox, del cual el usuario debe seleccionar alguno e inmediatamente después se mostrara la información asociada al empleado con ese código Tag, si ese el empleado que se desea dar de baja de la base de datos basta con hacer click en el botón Eliminar el cual ejecuta el siguiente código previamente explicado el cual ejecuta una sentencia DELETE.

```
private void button1_Click(object sender, EventArgs e)

{

string cadena = @"Data Source =.\SQLEXPRESS; initial catalog = Northwind;
Integrated Security=true";
SqlConnection conexion = new SqlConnection(cadena);
string queryinsert = "DELETE FROM Employees WHERE EmployeeID =
@EmployeeID";
SqlCommand cmd = new SqlCommand(queryinsert, conexion);
int eliminado = 0;
label1.Visible = true;
```

```
cmd.Parameters.AddWithValue("@EmployeeID", txtIDEmpleado.Text);

try
{

conexion .Open ();
eliminado = cmd.ExecuteNonQuery();
label1.Visible = true;
label1.Text = eliminado.ToString() + " " + "Registro Eliminado";
}
catch (Exception err)
{
label1.Text = "Error al Tratar de Eliminar el Registro";
label1.Text += err.Message;
}

finally

{
conexion .Close ();
}
}
```

8.7 Probando la Aplicación

Para probar la aplicación se debe tener conectado el lector a la PC mediante el cable USB e instalar sus drivers.

Ejecutamos nuestra aplicación e inmediatamente después podemos pasar una etiqueta RFID sobre el lector, y al instante la aplicación mostrara los datos del empleado asignados con ese ID de dicha tag.

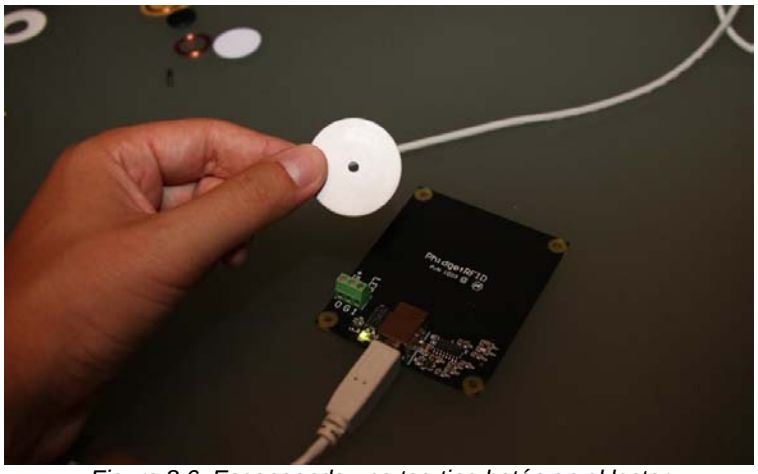


Figura 8.6 Escaneando una tag tipo botón en el lector

Figura 8.7 Identificación de la tag escaneada

Si la tag es autenticada por el lector y esta asociada con un empleado de la base de datos el LED que posee el lector enciende, lo que nos indica que permite el acceso al inmueble, en una aplicación donde se cuente con torniquetes o chapas electrónicas este impulso se enviaría a la tarjeta RS232/RS485 para que a su vez enviara la indicación al torniquete o chapa electrónica para que se activara el paso.

Se coloco una figura en color verde la cual simula la luz verde de un torniquete de control de acceso.

La aplicación cuenta con una sección para que el administrador de la misma pueda dar de alta usuarios y asignar una ID de una tag a un empleado de la organización y así la próxima vez que desee ingresar a las instalaciones deberá escanear la tarjeta y la aplicación despliegue sus datos en pantalla.

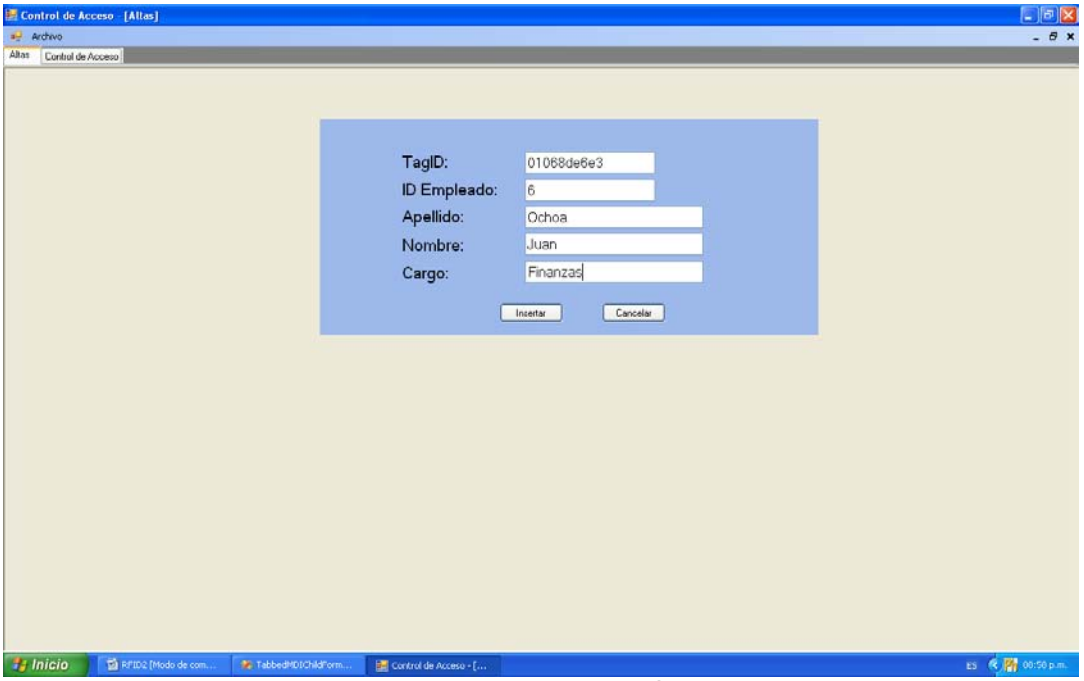


Figura 8.8 Dando de alta a un empleado asignándole una Tag especifica

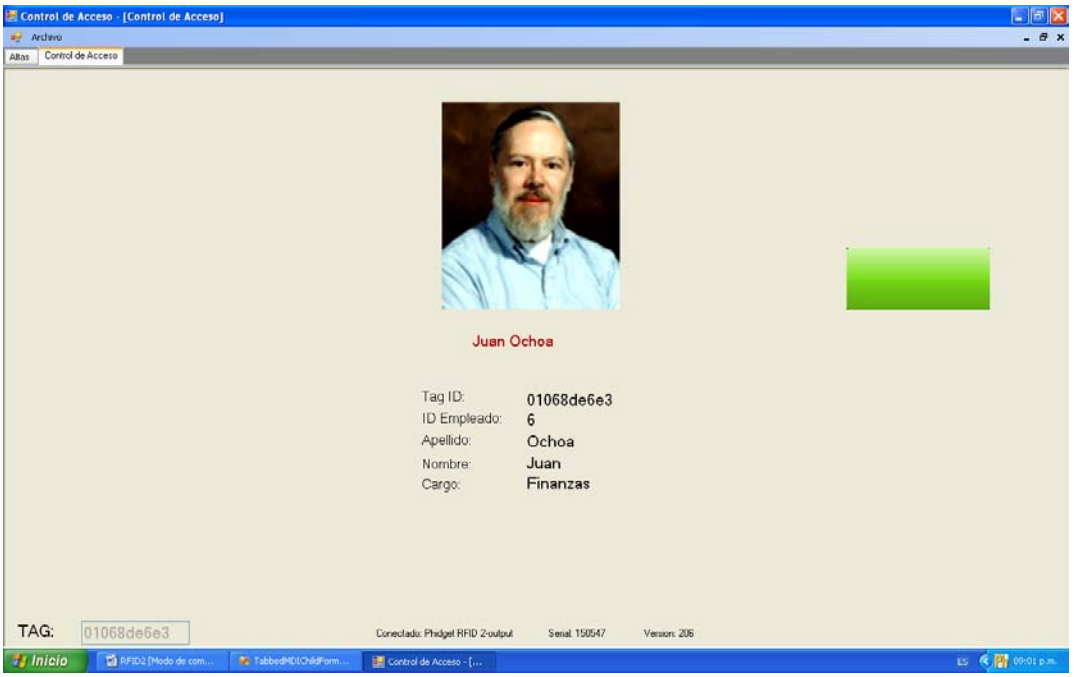


Figura 8.9 Ahora se lee la Tag dada de alta con anterioridad

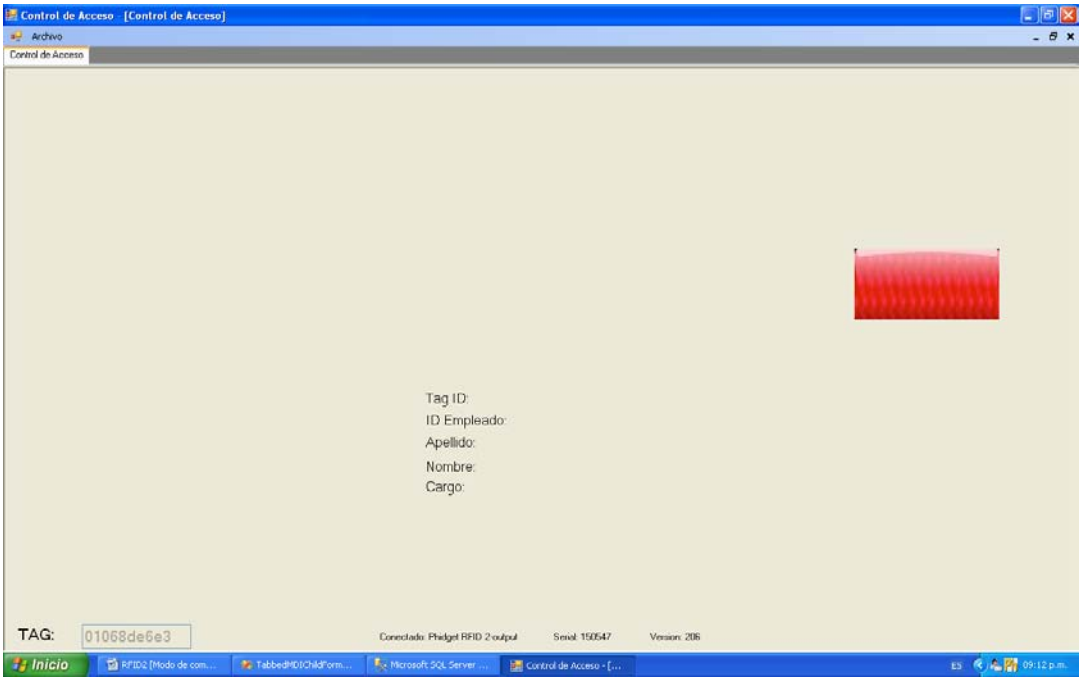


Figura 8.10 Escaneando una Tag no registrada en la Base de Datos

En caso de desplegar una Tag no registrada en la base de datos sobre el lector la aplicación leerá su código sin embargo los controles no mostraran información alguna y si mostrara la etiqueta roja de no acceso.

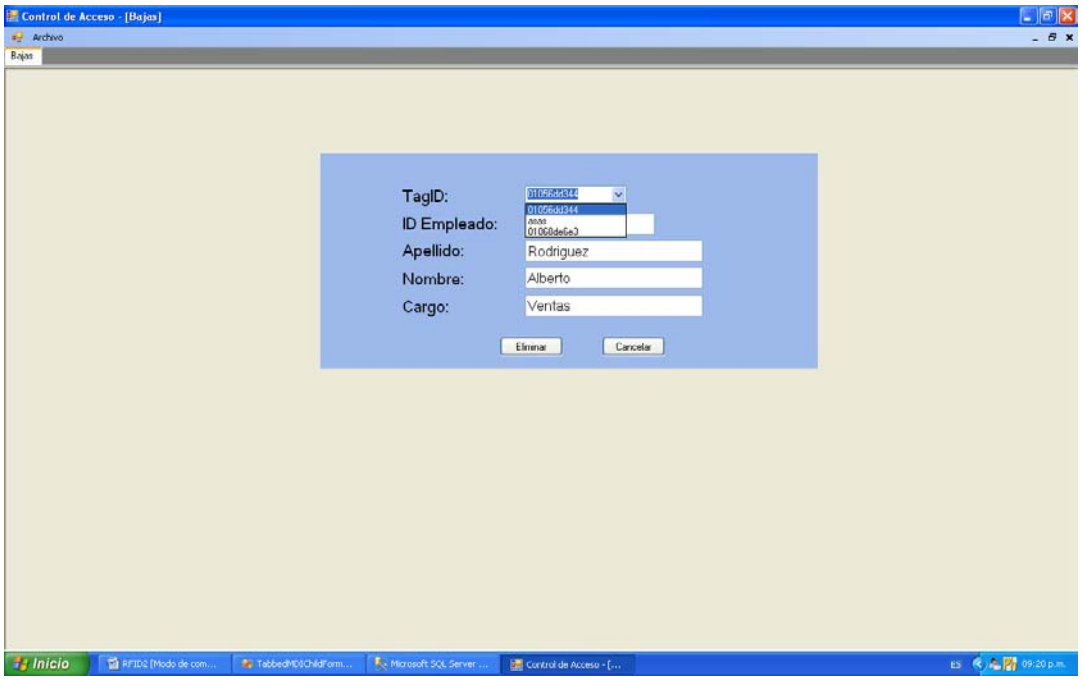


Figura 8.11 Dando de baja un usuario registrado

Para dar de baja un usuario registrado el cual tenga asignado una Tag para ingresar a las instalaciones se debe seleccionar el código Tag asignado a dicho usuario desde el combo box y dar click en el botón Eliminar

Si se desea se puede ver todos los empleados registrados en la tabla que almacena su información incluyendo el código Tag de la tarjeta asignada a cada uno de ellos.

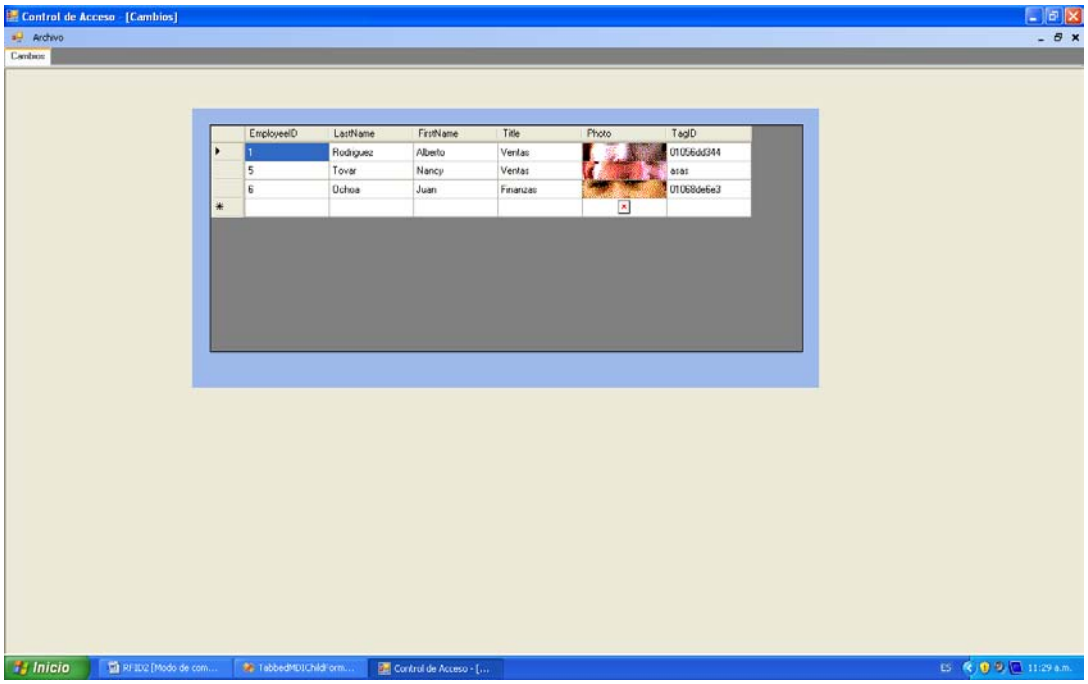


Figura 8.12 Vista de todos los registros

Trabajo Posterior

En este trabajo se utilizaron dispositivos que trabajan en baja frecuencia (125Khz) tanto el lector como las etiquetas. En la actualidad es la frecuencia más utilizada para este tipo de sistemas por el bajo costo de los dispositivos, principalmente en las tarjetas que a nivel masivo hablando de una empresa o escuela puede resultar un gasto importante.

Sin embargo se recomienda utilizar dispositivos HF (13.56 MHz) para controlar el acceso de personas y para el acceso de vehículos se requieren dispositivos UHF.

Así mismo se debe contar con los siguientes componentes:

- Lectores RFID.- Para este módulo se debe buscar una ubicación próxima a la computadora desde la cual se va a gestionar el sistema RFID y protegida de manera que no se tenga acceso a ella fácilmente. La ubicación de este dispositivo no define la cobertura del sistema, ya que la antena que contiene el lector, la cual, de acuerdo a su patrón de radiación define la cobertura del sistema. Por esta misma razón el alcance puede ser variado hasta cierto punto. Para las entradas y salidas de las Instalaciones al aire libre se recomienda la instalación de lectores empotrables en la pared de 13.56 MHz que pueden enviar la señal a torniquetes metálicos mediante una tarjeta RS232/RS485. Cabe mencionar que existen torniquetes diseñados para este tipo de aplicaciones los cuales cuentan con lectores de RFID incrustados en la parte superior del mismo y cuentan con una tarjeta controladora que interactúa con la tarjeta RS232/RS485 que concede o no el acceso al personal y soportan las inclemencias del clima.

  Si se contempla la instalación en instalaciones cerradas se puede optar por una infinidad de lectores para todo tipo de accesos ya sean puertas metálicas, de madera, o simplemente un lector que permita la lectura de una tarjeta e indique la autenticidad del individuo en un monitor LCD.

  El módulo provee de todas las funciones de radiofrecuencia y control para comunicarse con los transponders, este envía la señal energizante al transponder, modula la señal RF para enviar los datos al transponder, decodifica y analiza los datos recibidos del transponder y los trasmite por la interfaz estándar serial (RS232 o RS422/485).

- Estación Principal.- Computadora en la cual se manejan tres funciones principales al mismo al mismo tiempo, gestionar el módulo RFID a través del puerto serial, comunicación

con los servidores que contienen las bases de datos y mostrar los resultados de la aplicación.

Teniendo en cuenta otras aplicaciones que deban correr al mismo tiempo con el sistema de registro y control de salida de elementos mediante dispositivos RFID, el equipo debe cumplir con ciertos requerimientos mínimos de hardware, procesador Pentium III a 1GHz, RAM de 512Mb, tarjeta de red, un puerto serial disponible y capacidad de manejar video con resolución de 800 x 600 píxeles. El software requerido es el sistema operativo Microsoft Windows XP o mas reciente y Microsoft SQL Server cliente.

- Punto de Red Establecido.- Un punto de red habilitado en la entrada principal de las Instalaciones para asociarse a la red local con el fin de comunicar la estación principal con los servidores que contienen las bases de datos del personal.

- Servidores.- Equipos servidores que mantienen las bases de datos de la organización. Se recomienda tener Microsoft Windows Server Versión 2003. Además se requiere de un servidor único destinado a la Aplicación RFID que tenga acceso a los demás servidores todo esto con el fin de pedir la información necesaria a los servidores que mantienen las bases de datos de la organización y mantener dichos servidores a salvo de posibles inconvenientes que pudieran afectar a otras aplicaciones de la organización

- Tags.- Aquí depende mucho del control de acceso que se requiera, es decir si solo se requiere controlar el acceso del personal o también de los vehículos, y del tamaño de las instalaciones. Sin embargo se recomienda el uso de tags de 13.56 MHz de lectura y escritura tanto para el personal como para vehículos siempre y cuando las finanzas de la organización lo permitan.

En cuanto al desarrollo de la aplicación el siguiente paso seria desarrollar una aplicación que se adapte al 100% a las necesidades de la organización es decir gestionar las tarjetas del personal y de los vehículos. Tener varios módulos como pueden ser la configuración del sistema mediante un administrador, que a su vez tenga un modulo de escritura en las tags para distintos modelos y fabricantes de tarjetas, generación de reportes del numero de entradas y salidas del personal por hora, día, semana, etc. Así mismo que permita dar de baja tags y se bloquee la misma para negar el acceso a una persona o vehiculo en fin todo dependería de las políticas de control de acceso que se manejen. Inclusive se pudiera aprovechar esta misma aplicación para manejar la elaboración de horarios de trabajo, salidas al comedor, tolerancia de tiempos, etc.

Inclusive y muy importante que se desarrollara un modulo para la entrada de visitantes que almacenará fotografías tomadas a los mismos mediante una cámara Web instalada en las entradas de las instalaciones y la asignación de una tag provisional que le permitiera el paso.

En caso de que las instalaciones de la organización cuenten con cafeterías o comedores pudiera aprovecharse esta aplicación para realizar un modulo para el manejo de monedero electrónico para pequeñas compras en los mismos.

Seria muy importante que la aplicación sea totalmente distribuida y que sea Web ya que este tipo de aplicaciones están siendo el patrón en los últimos años debido a la aparición de lenguajes de programación que permiten la fácil creación de estas aplicaciones, en realidad hoy en día una aplicación que no sea Web esta totalmente destinada al fracaso.

Es muy recomendable desarrollar la aplicación en ASP.Net aprovechando el código ya existente, además de Ajax y XML.

Cabe señalar que un sistema de este tipo debe estar disponible 24x7, y se deben contemplar las fallas en el mismo es por tal motivo que se debe contemplar tener un Host con respaldo.

Conclusiones

A lo largo de estos capítulos hemos visto cómo la tecnología RFID ha dejado de ser una tecnología prometedora para hacerse realidad, postulándose como una tecnología de amplias posibilidades de utilización en casi cualquier ámbito.

Prácticamente todos los estudios realizados muestran preferencia de RFID sobre el código de barras, aún siendo estos últimos más baratos que las etiquetas. De hecho, la tecnología RFID resulta ser más eficiente en términos de costo, gracias al valor añadido que supone la facilidad y rapidez en la lectura y su mejor integración con los sistemas de información existentes, infiriendo todo esto en un ahorro de tiempo del personal dedicado a tareas fácilmente automatizables, así como la minimización de las pérdidas y de los errores.

Además, la integración es especialmente sencilla con la estructura de comunicaciones inalámbricas (posiblemente) desplegada en cualquier lugar donde se piense implantar un sistema RFID. Por tanto, los inversionistas deben ampliar miras y analizar la situación de este modo, no esperando un retorno de la inversión a corto plazo, sino más bien a medio plazo.

Cabe destacar que no se prevé que la tecnología RFID sustituya o elimine por completo al código de barras, sino que serán dos tecnologías que coexistirán en el tiempo. En primer lugar, porque aún no existe un estándar único a nivel mundial, como ocurre con los códigos de barras, y en segundo lugar porque actualmente RFID no es la solución idónea para cualquier producto. Por ejemplo, en la industria farmacéutica, hay sustancias que contienen líquidos, por lo que la señal puede verse alterada. Esto significa que mientras no se encuentre una solución, se seguirá utilizando el código de barras para éstos productos.

Otra razón de peso es el costo. Sigue resultando cara la implantación masiva y mientras los inversionistas no aprecien un evidente retorno de beneficios, o aparezca algún driver de mercado que fomente su implantación, será difícil alcanzar un despliegue a gran escala. Sin embargo, no debemos olvidar que RFID posibilita un modelo de negocio mucho más amplio que el código de barras.

Otra de las ventajas que aporta RFID frente a otras tecnologías es su capacidad para, sólo o en cooperación con la infraestructura inalámbrica existente en las instalaciones donde se desee instalar, poder realizar el seguimiento de todos aquellos objetos etiquetados, de cualquier tipo Esta aplicación viene despertando un creciente interés, ya que los problemas logísticos en un centro que debe gestionar tanto personal como activos y equipos, son enormes.

.

En lo concerniente a la legislación como se sabe México esta muy rezagado en el ámbito de la legislación sobre tecnología, contrario a otros países o bloques como la Comisión Europea que ha propuesto durante 2007 una estrategia política común sobre las etiquetas RFID, para dar respuesta a las preocupaciones de los ciudadanos en relación a la protección de la privacidad, y tratar de impulsar de ese modo la confianza de los consumidores y fomentar la posición de Europa en un mercado que crece a un ritmo del 60% en todo el mundo.

Por otro lado, el uso masivo de la telefonía móvil entre la población junto con la posibilidad real de tener teléfonos móviles que incorporan dicha tecnología (por ejemplo, Nokia 6131 NFC) hacen necesaria una seria apuesta por la tecnología NF.

En lo concerniente al desarrollo de la aplicación fue una tarea delicada conseguir los dispositivos RFID ya que en nuestro país no existen empresas que provean este tipo de dispositivos al menudeo, y se tuvo que realizar un pedido directamente al fabricante.

Aunque en nuestro país existen empresas que desarrollan e implantan este tipo de soluciones a precios sumamente elevados, el haber importado los dispositivos RFID utilizados para este trabajo no elevo los precios de manera considerable como se pensaba.

Con este trabajo cualquier estudiante, profesor o investigador en la materia puede tener un gran panorama de lo que es la Identificación por radio frecuencia complementado con la aplicación que se desarrollo, la cual puede servir como base para futuros trabajos, la mejora de la misma o simplemente para realizar lecturas a Tags que cumplan con norma EM4102

En lo personal fue una gran experiencia haberme adentrado en este tipo de tecnologías y tener una visión de lo que se puede realizar con esta tecnología. Así mismo me deja la inquietud de pensar en lo que viene relacionado a la RFID en un futuro no muy lejano, quizás no en nuestro país ya que aquí el uso de la RFID apenas comienza teniendo solo dos aplicaciones de uso masivo como lo es las tarjetas de acceso para el Sistema de Transporte Colectivo (STC-Metro) que es una solución de control de acceso a los andenes del metro de la Ciudad de México, la otra es muy similar y son las tarjetas de acceso a las inmediaciones de las estaciones del Metro bus también en la Ciudad de México. Estos dos ejemplos sirven como ejemplo para visualizar el uso importante que tiene la RFID en la vida cotidiana de las grandes ciudades. Sin embargo esto puede ir mas alla aprovechando la infraestructura de las redes de la telefonía móvil y el uso masivo de la misma se pueden realizar e implantar aplicaciones muy potentes complementando la RFID con NF.

Glosario

ARPANET (Advanced Research Projects Agency Network). Fue creada por encargo del Departamento de Defensa de los Estados Unidos ("DoD" por sus siglas en inglés) como medio de comunicación para los diferentes organismos del país. El primer nodo se creó en la Universidad de California, Los Ángeles y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP en 1983.

ANSI (American National Standards Institute, Instituto Nacional Estadounidense de Estándares). Organización que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).

ASIC (Application Specific Integrated Circuit, Circuito Integrado para Aplicaciones Específicas)

AUTO-ID CENTER Equipo de investigación del MIT (Massachussets Institute of Technology) dedicado al estudio de RFID.

BER (Bit Error Rate): La proporción del número de bits recibidos que son considerados erróneos del total de bits transmitidos.

CBC (Cipher Block Chaining) Uno de los modos de operación de una unidad de cifrado por bloques

CFB (Cipher Block Chaining) Uno de los modos diferentes de operación de una unidad de cifrado por bloques

CMOS (Complementary Metal Oxide Semiconductor, "Semiconductor de Metal Óxido Complementario") es una de las familias lógicas empleadas en la fabricación de circuitos integrados (chips). Su principal característica consiste en la utilización conjunta de transistores de tipo pMOS y tipo nMOS configurados de tal forma que, en estado de reposo, el consumo de energía es únicamente el debido a las corrientes parásitas.

CRC (Cyclic Redundancy Check): Algoritmo de detección de errores que explota las ventajas del módulo-2 aritmético para generarlo.

Db. Decibelio es la unidad relativa empleada en acústica y telecomunicaciones para expresar la relación entre dos magnitudes, acústicas o eléctricas, o entre la magnitud que se estudia y una magnitud de referencia.

EAN (European Article Number): Es el principal estándar de código de barras.

EAS (Electronic Article Surveillance): Sistemas basados en un único bit de información en los transponders, usado principalmente como sistema antirrobo en almacenes y establecimientos.

ECB (Electronic Codebook) Es uno de los modos de operación de una unidad de cifrado por bloques

EEPROM (Electrically Erasable Programmable read-only memory): Memoria más usada en los sistemas con acoplamiento inductivo. Tiene unos ciclos de escritura limitados y un consumo alto de batería.

EIRP (Effective Isotropic Radiated Power) El producto de la potencia de entrada de la antena y la ganancia relativa a una fuente isotrópica.

EPC Siglas de Código Electrónico de Producto (Electronic Product Code).

EPC-IS (EPC Information Services) Ha sido diseñado para actuar como una "Internet de los productos" que permitirá a los socios de negocio conocer la información de los productos en los diferentes momentos de la cadena de abastecimiento, de manera permanente y en tiempo real.

ERP (Enterprise resource planning, planificación de recursos empresariales). son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios.

FCC (Federal Communications Commission, Comisión Federal de Comunicaciones) Agencia estatal independiente de Estados Unidos, bajo responsabilidad directa del Congreso. La FCC fue creada en 1934 con la Ley de Comunicaciones y es la encargada de la regulación (incluyendo censura) de telecomunicaciones interestatales e internacionales por radio, televisión, redes inalámbricas, satélite y cable.

FIPS (Federal Information Processing Standards, Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSI, IEEE, ISO, etc.)

FRAM (Ferromagnetic Random Acces Memory): Memoria usada en sistemas de RFID más complejos que posee mejor tiempo de escritura y mejor consumo que la memoria EEPROM.

Full Duplex (FDX) Canal de comunicaciones que permite la transmisión de datos en ambas direcciones al mismo tiempo.

Half Duplex (HDX) Canal de comunicaciones que permite la transmisión de datos en ambas direcciones pero no al mismo tiempo.

FHSS (Frequency Hopping Spread Spectrum) La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada dwell time e inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

IFF (Identification Friend or Foe, Identification Amigo o Enemigo). Sistema de Identificación electronico por radio

ISM (Industrial, Scientific and Medical) son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en areas industrial, científica y médica.

LED (Light-Emitting Diode, Diodo Emisor de Luz) Dispositivo semiconductor (diodo) que emite luz incoherente de espectro reducido cuando se polariza de forma directa la unión PN del mismo y circula por él una corriente eléctrica.

Mifare. Tecnología de tarjetas inteligentes sin contacto (TISC) más ampliamente instalada en el mundo

Modulación Backscatter: Proceso donde el transponder responde a la señal del lector, modulando y retransmitiendo una señal con la misma frecuencia portadora.

NFC (Near Field Communication) Protocolo basado en una interfaz inalámbrica. La comunicación se realiza entre dos entidades (peer-to-peer). El protocolo establece conexión wireless entre las aplicaciones de la red y los dispositivos electrónicos.

P2P (Per To Per). Red de pares, es una red de computadoras en la que todos o algunos aspectos de esta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre si. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

RA. Siglas de Random Access Memory. Memoria de acceso aleatoria y volátil.

RF. Abreviatura de Radiofrecuencia

RFID (Radio Frequency IDentification): Sistema de identificación automática y capturadora de datos que comprende uno o más lectores y uno más transponders que realizan la comunicación a determinada frecuencia.

ROM Siglas de Read Only Memory. Se trata de memoria de sólo lectura.

SRAM (Static Random Acces Memory): Memoria más utilizada en los sistemas RFID de microondas. Mejor ciclo de escritura a cambio de un suministro de energía continuo por una batería auxiliable.

SSR (Secondary Surveillance Radar, Radar Secundario de Vigilancia). Sistema que permite la identificación y seguimiento de blancos específicos en el espacio, generalmente aeronaves.

SOC (System on a chip, Sistema en chip)

TAG término sinónimo a transponder, usado especialmente por la AIM

UWB (Utra Wide Band) se usa para referirse a cualquier tecnología de radio que usa un ancho de banda mayor de 500 MHz o del 25% de la frecuencia central, de acuerdo con la FCC

WMS (Warehouse Management System, Sistema de administración de Almacen) Softwre dedicado a manejo de entradas y salidas y cualquier movimiento de materia prima en almacenes

Bibliografía

[2] Patrick J. Sweeney II, *RFID for Dummies* ,Wiley Publishing, Inc., 2005.Páginas 90-98

[3] Bhuptani, Manish; RFID Field Guide: Developing Radio Frecuency Identification Systems; Second Edition, Prentice Hall, USA, Chicago. 2004, Páginas 210-223

[4] Informe de IDTechEX. Septiembre de 2006

[5] *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification,Second Edition,* Klaus Finkenzeller. Copyright 2004 John Wiley & Sons.Páginas 150-152

[6] Pete Sorrells, "Passive RFID Basics", Microchip Technology Inc

[7] *RFID A Guide to Radiofrequency Identification*, V. Daniel Hunt, Albert Puglia, Mike Puglia,Wiley Interscience, 200,Páginas 50-62

[8] RFID in Action http://www.rfidinaction.net/

[9] *RFID A Guide to Radiofrequency Identification*, V. Daniel Hunt, Albert Puglia, Mike Puglia,Wiley Interscience, 2007,Páginas 11-38

[10] RF 5152, RF Micro Devices, Inc., http://www.rfmd.com

[11] Pete Sorrells, "Passive RFID Basics", Microchip Technology Inc, Página 40-49

[12] Lahiri, RFID Spurcebook; First Edition; Prentice Hall – IBM Press, USA 2006, Páginas 110-142

[13] RF 5152, RF Micro Devices, Inc., http://www.rfmd.com

[14] ERA 3, Mini-Circuits, http://www.minicircuits.com

[15] Godínez, Miguel; RFID: Oportunidades y riesgos, su aplicación práctica; Primera Edición, Alfaomega, México, D.F. 2007, Página 48

[16] Hunt, Daniel, Puglia, Albert Puglia, Mike; RFID: A guide to Radio Drecuency Identification: Firts Edition, Hardcover, USA, New Cork. 2006,Páginas 201-226

[17] *EPC Tag Data Standards Version 1.1 Rev. 1.24., Standard Specification 01,* April 2004. EPCglobal Inc

[18] Sanghera, Paul; RFDI+; Elsevier Books, Oxford, USA. 2007, Páginas 155-156

[19] IDTrack – Sure Identifiation & Traceability http://www.rfidc.com/docs/about.htm

[20] Yoshihisa, T. Kishino, Y. Terada, T. Tsukamoto, M. Sagara, R. Sukenari, T. Taguchi, D. Nishio, S. *A rule-based RFID tag system using ubiquitous chips* Osaka Univ., Japan: Active Media Technology, 2005. (AMT 2005). Proceedings of the 2005 International Conference on, 19-21 May 2005,Páginas: 423 – 428.

[21] N. Bradshaw, V. Hague, M. Raza*, Applications of RFID technology* Microlise Syst. Integration Ltd.: RFID Technology (Ref. No. 1999/123), IEE Colloquium on, 25 Oct. 2006 páginas: 119 - 121

[22] Klaus Finkenzeller. *RFID Handbook: Fundamentals and aplications in Contactless Smart Cards and Identi¯cation*, John Wiley Sons,Ltd. 2005. 419pgs.

[23] Hahnel, D. Burgard, W. Fox, D. Fishkin, K. Philipose, *Mapping and localization with RFID technology,* Hahnel, D. Burgard, W. Fox, D. Fishkin, K. Philipose, M. Dept. of Comput. Sci., Freiburg Univ., Germany, Robotics and Automation, 2006. Proceedings. ICRA '04. 2004 IEEE International onference on Publication Date: 2004 Volumen:1,páginas: 1015 - 1020.

[24] John R. *Traditional And Emerging Technologies And Applications In The Radio Frequency Identification (Rfid) Industry*. Tuttle Micron Communications, Inc.2004 IEEE Radio Frequency Integrated Circuits Symposium

[25] Active Tag RFID Tecnhnovelgy. http:// www.technovelgy.com/Visitada Mayo 2006.

[26] Berthon, A. & Guillory, M., 2005. Security in RFID. Texas Instruments and Intermec Technologies. http://stud.ita.hsr.ch/ss03/ss0304/

[27] Juels, A., 2007. Minimalist Cryptography for Low-Cost RFID Tags. RSA Laboratories, Bedford, USA

[28] Sarma, S., Weis, S., and Engels, D, 2005. RFID Systems, Security & Privacy Implications. Auto-ID center Massachusetts institute of technology, Cambridge, USA.

[29] Juels, A., 2006. Strengthening EPC Tags Against Cloning. RSA Laboratories, Bedford, USA.

[30] RFID Wizards
http://rfidwizards.com/index.php?option=com_content&view=article&id=242:iso-rfid-standards-a-complete-list&catid=227:standards

[31] RFID Journal http://www.rfidjournal.com/article/print/1335

Sitios Web de Interés Consultadas

• NFC Forum
Sitio web sobre NFC
http://www.nfc-forum.org/aboutnfc/

• Directorio RFID
Sitio web con información sobre empresas españolas del mercado RFID
http://directoriorfid.com/

• Sitio web de la Comisión Europea
Descripción de las políticas y actividades de RFID dentro de la UE.
http://ec.europa.eu/information_society/policy/rfid/index_en.htm

• RFID Consultation Website
Sitio web que muestra los resultados de la Consulta Pública sobre RFID, así como noticias, eventos e iniciativas de interés dentro de la CE.
http://www.rfidconsultation.eu/
• RFID security &Privacy

Sitio web con información sobre publicaciones e informes relacionados con la seguridad y privacidad en RFID
http://www.avoine.net/rfid/

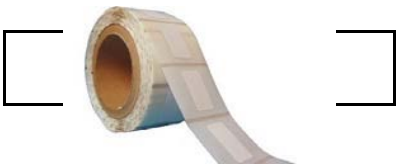
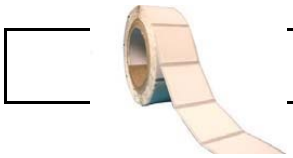
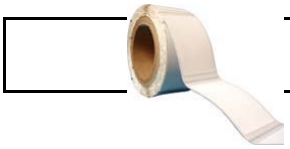
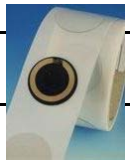
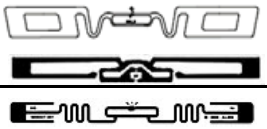
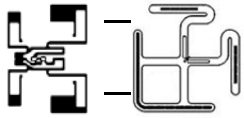
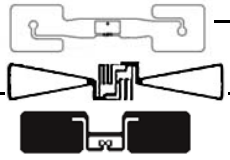
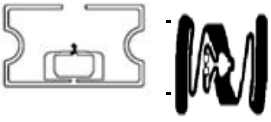
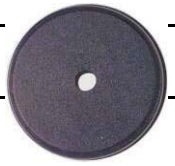
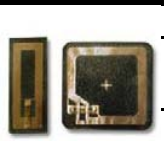
• Requirements and options for Actions in RFID in Healthcare
Call for Tenders del VIIPM que cerró en Septiembre de 2007.
http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsTenderPage&call_id=67.

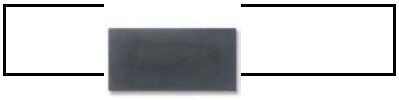
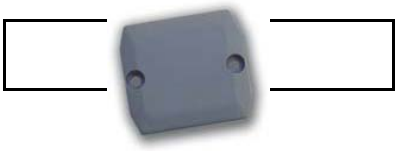
• The Independent European Centre for RFID, Wireless and Mobility
http://www.rfidc.com/docs/about.htm

• Gartner Consulting
http://www.gartner.com/

Anexos

Algunos tipos de Tags RFID disponibles en el mercado para casi cualquier tipo de gestión de objetos.

Etiqueta Adhesiva P-Label ISO- HF	Etiqueta Adhesiva P-Label ISO- HF	Etiqueta Adhesiva P-Label ISO- HF
		
Etiquetas de papel blancas, adhesivas e imprimibles.Memoria: 1024 bits o más	Etiquetas de papel adhesivas e imprimibles. Ideales para libros y doctos.Memoria: 1024 bits o más	Etiquetas de papel blancas, adhesivas e imprimibles, tamaño tarjeta. Memoria : 1024 bits o más.
Etiqueta Adhesiva P-Label ISO- HF	**Line Tag EPC- UHF**	**Square Tag EPC- UHF**
		
Etiquetas circulares adhesivas e imprimibles, con orificio central. Ideal para cd's. Memoria: 1024 bits o más	Tags adhesivos sin sustrato de papel, Polarización lineal. Máxima distancia de lectura. Memoria: 96 bits + 240 bits	Tags adhesivos sin sustrato de papel. Alto rendimiento e insensibles a la orientación (3D). Memoria: 96 bits
Global Tag EPC-UHF	**Miní Tag EPC-UHF**	**Light Tag EPC-UHF**
		
Tags adhesivos sin sustrato de papel. Gran ancho de banda, para la mayoría de aplicaciones. Memoria: 96 bits	Tags adhesivos sin sustrato de papel, Ideal para identificación de corto alcance, a nivel artículo. Memoria: 96 bits	Tags adhesivos sin sustrato de papel (inlays), Gran rendimiento y memoria adicional para el usuario. Memoria: 96 bits+ 240 bits
Logi Tag ISO-LF/HF	**World Tag ISO- LF/HF**	**Tag Adhesivo para metal EPC- UHF**
		
Tag circular encapsulado de reducido tamaño y distancia de lectura optimizada. Lectura hasta 30cm iCode SLI, Mifare, Unique	Tag circular encapsulado con un orificio central para su fijación. 125Khz o 13,56Mhz iCode SLI, Mifare, Unique	Tag flexible de ferrita diseñado para ser adherido a materiales metálicos.Memoria: 1024 bits Lectura hasta 100cm

Metal Tag R30 ISO-LF/HF	Blue Tag Standard EPC- UHF	Blue Tag onmetal EPC- UHF
		
Tag circular encapsulado diseñado para ser adherido a materiales metálicos. 125Khz o 13,56Mhz iCode SLI, Mifare, Unique	Tag UHF rígido capaz de soportar condiciones atmosféricas y agentes químicos. Lectura hasta 3-4 m (1-2 en presencia de metales o líquidos)	Tag UHF rígido para metal capaz de soportar condiciones atmosféricas y agentes químicos. Lectura hasta 3-4m Agujeros para fijación
Super Rugged Tag ISO-LF	**Super Rugged Tag EPC-UHF**	**Tag Inyección de Plástico ISO-HF**
		
Tag de alta robustez, capaz de soportar condiciones extremas de presión, temperatura y humedad. Memoria: 1024 bits Lectura hasta 100cm ISO15693, iCode SLI	Tag de muy alta resistencia y durabilidad , para montaje sobre superficies metálicas. Lectura hasta 3-4m EPC Class1 Gen2	Tag preparado para su inyección en materiales de plástico, formando parte íntegra de estos tras su fabricación
Tag Lente D5 ISO-HF	**Tarjeta Pástica ISO-LF/HF**	**Tarjeta Blue Card EPC/ ISO-UHF**
		
Tag robusto con forma de lente para fijación en materiales metálicos.Memoria: 2 kbits Lectura hasta 5 mm ISO 15693-2	Tarjeta plástica de larga durabilidad para uso diario. Ideal para control de accesos. Imprimible.Lectura hasta 150cm	Tag UHF en formato tarjeta, para aplicaciones de control de accesos y seguimiento de cajas. 96bit ID + 128bit Lectura hasta 3m
Blue Card Combinada EPC/ISO-HF/UHF	**AVI Label EPC-UHF**	**Tag AVC EPC/ UHF**
		
Tarjeta de tecnología dual UHF y Mifare 1S50, para lecturas combinadas de corta y larga distancia. Lectura hasta 2m (UHF) o proximidad	Etiquetas con impresión a dos caras, para adherir en la luna de vehículos. 512 bits Lectura hasta 4-5m	Tarjeta para el sistema NPS Express-ID Lite, diseñado para monitorizar contenedores, vehículos o personas.2.45 Ghz Lectura hasta 8 m

Hi Card Tag 2	Pulsera RFID ISO-HF	Pulsera RFID SC ISO-HF
		
Tag de tamaño reducido del sistema NPS Hi-Track 2, con pulsador para forzar la identificación. 2.45Ghz + 433Mhz Lectura hasta 15 m o 40m con pulsador	Pulsera RFID con clip de seguridad permanente.	Pulsera RFID de cierre adhesivo para detección de sustracción.
Pulsera RFID Silicón ISO-HF	**Llavero RFID ISO-LF/HF**	**Micro Tag ISO-HF**
		
Pulsera de silicona con tag RFID incorporado. Disponibles varios colores. Memoria: 1024 bits	Tag integrado en llavero RFID. 13.56 MHz	Tag diminuto para la identificación de cualquier elemento. Memoria: 16 Kb Lectura hasta 3 mm
Glass Tag ISO-LF	**Cyl Tag ISO-HF**	**Phone Tag ISO-HF**
		
Tag de vidrio de 13mm para la identificación de pequeños elementos.	Tag con encapsulado cilíndrico de nylon para ubicaciones específicas Lectura a 60mm	Tag adhesivo antideslizante para teléfonos móviles. Color y logotipo personalizable. Memoria: 1024 bits o más
Ham Tag ISO-HF	**Tag Screw P ISO-HF**	**Brida con Tag externo ISO-HF**
		
Tag específico para carnes y paletillas, diseñado para soportar los procesos por los que pasan estos alimentos. Memoria: 896 bits + 64 bits	Tag en formato tornillo de plástico. 2048 bits	Brida con tag removible encapsulado en epoxy. 2kb Lectura hasta 20mm

Cable Tag ISO-HF	Active Compact Tag EPC-UHF	Active Tag 100m c/localizador EPC
		
Tag de PVC diseñado para sujección con brida o cable, encapsulado y waterproof.13.56 Mhz Lectura hasta 50mm	Tag del sistema NPS ActiveTrack-2 en versión ultra-fina para adherir a objetos. Lectura hasta 90 m Opc.: sensor de movimiento	Tag del sistema NPS ActiveTrack-2 para mayor precisión de localización, con sensor de movimiento. Lectura hasta 90 m Opc.: sensor antivandálico y/o pulsador
Textil Tag ISO-HF	**Textil Tag C ISO-HF**	**Texti Tag T EPC-HF/UHF**
		
-20°C a +95°C / Parcheado de hasta 10 sek. a 210°C;Ultra-plano. Memoria: 2 Kbits	Tags cerámicos para lavanderías. 864bit Lectura hasta 40cm	Etiqueta textil con tag ISO o EPC Gen2 integrado. Lavable y con textura de tela. Memoria: 96 bits o más
Textil Tag P EPC-UHF	**LT Tag EPC-UHF**	**Tag ThermRF Logger ISO-HF**
		
Tag plano y flexible diseñado para soportar lavado, planchado y secado. 96 bits Lectura hasta 2 m	Tag UHF semipasivo capaz de registrar temperatura y tiempo a intervalos de 8 segundos. Mem. 17 KByte Lectura hasta 10m	Tag 100% impermeable, capaz de almacenar periódicamente información de temperatura con elevada precisión. Memoria: 346 bits 12 meses en operación continua